2020年上半年度 手机安全状况报告

360手机卫士
360企业安全
中国信息通信研究院
联合发布

360手机卫士 360政企安全 CAICT 中国信通院 360安全大脑

VISIT…

LANZAROTE
Caliente.COM

扫码免费领取资料



房中术(www.nblax520.com)专注于男性增大增粗增长、阳痿、早泄、壮阳、延时、强肾、回春、健身。女性缩阴、丰胸、减肥、化妆、瑜伽、保养、产后修复、盆底肌锻炼。两性健康,夫妻按摩,房中术,性姿势,性技巧,性知识等

更多免费教程：英语学习，技能提升，PS 教学，投资赚钱，音乐教程，口才教学，情商提升，风水教学，心理学，摄影知识，幼儿学习，书法学习，记忆力提升等等......

扫码加微信lax988988领取资料



==

全站课程下载

课程不断增加

本站现资源容量已超 10T

入群联系 QQ：167520299 或添加微信：1131084518（备注 学习）

阳痿早泄训练
皇室洗髓功视频教学
女人驻颜术
泡妞约炮万元课程
足疗养 SPA 教材
玉蛋功
马氏回春功
房中术张丰川
哲龙全套视频
增大盼你增大
国际男优训练
亚当德永早泄训练
洗髓功真人内部
皇室养生绝学道家洗髓功
【铁牛人会员课】男人必备技能，理论讲解
实战高清视频
随意控制射精锻炼 视频+图片+文字
价值 1440 元第一性学名著<素女经房中养生
宝典视频>12 部
洗髓功修炼方法视频教学
陈见玉蛋功视频教学 女性缩阴锻炼
男性自然增大增长指南
强性健肾保健操 1-4
道家强肾系统锻炼功法
马氏回春功
12 堂课，全面掌握男性健康问题 让你重燃自信
联系微信：1131084518

1、东方性经
2、印度 17 式
3、口交技巧 3 部
4、港台性姿势 3 部
5、365 性姿势 6 部
6、泰国性爱密经 17 式
7、花花公子性技巧 6 部
8、阁楼艳星性技巧 7 部
9、古今鸳鸯秘谱全集 7 部
10、夫妻爱侣情趣瑜伽 2 部
11、古代宫廷性保健系列 14 部
12、汉唐宋元明清春宫图真人
13. 柔软性爱宝典 日本 9800 课
14. 李熙墨 3999 全套课
15. 妖精性爱课 2888
16. 李银河全套性课
17. 领统统性课
18. 德勇男性篇
19. 德勇男性篇
20. 缓慢性爱
21. 亚当多体位搭配篇
22. 亚当多体位结合篇
23. 德勇克服早泄讲座练习
24. 德勇以女性为中心得爱抚
25. 加藤鹰接吻爱抚舌技
26. 加藤鹰指技
27. 加藤鹰四十八手入门
28. 佐藤潮吹教学
29. 佐藤男人体能锻炼+保健品介绍
30. 佐藤男人早泄对抗训练
31. 阿拉伯延时训练
32. 田渊正浩秘籍
33. 异性性快感集中训练教学
34. 自我愉悦锻炼密宗
35. 铁牛全套延时训练课
36. Pc 机锻炼真人视频教学
37. 印度性经全集 8 部
38. 21 世纪性爱指南
39. 香蕉大叔男女训练馆全套
40. 中美真人性治疗教学+理论
41. 女性闺房秘术
42. 幸福玛利亚性课
43. 陈见如何释放性魅力征服
44. 性爱技巧讲座全套
45. 性爱秘籍全套
46. 性爱误区讲座
47. 性病讲解大全
48. 性博士讲座合集
49. 性健康和性高潮合集
50. 性教育讲座合集
51. 性能力课堂合集
52. 性生活问题解析合集
53. 意外怀孕和避孕处理课堂
54. 性感地带探索
55. 性技巧讲座
56. 性健康与性卫生讲座
57. 性生活专家答疑
58. 性心理与性道德合集
59. 性爱宝典合集
60. 性爱技巧合集
61. 完美性爱演示
62. 完美性爱技术讲解
更多精品等你来解锁哦...........

每日免费获取报告

1、每日微信群内分享7+最新重磅报告；

2、每日分享当日华尔街日报、金融时报；

3、每周分享经济学人

4、行研报告均为公开版，权利归原作者所有，起点财经仅分发做内部学习。

扫一扫二维码
关注公号
回复：研究报告
加入“起点财经”微信群。。



前言

我国通信技术的突飞猛进，间接提升了用户的网络体验，数字信息化为大众生活带来了诸多便利，为企业发展奠定了基础。为推动通信技术服务的发展，各类高效传播渠道应运而生，帮助企业在进行产品的推广及宣传时能够以极强的针对性直达目标客户，在快速传播的同时还降低了成本，满足了各大企业的传播需求。但是由此而引发出的各渠道号段遭到不法分子利用等现象，在某种程度上也加剧了骚扰及诈骗事件的发展。

受到新冠肺炎疫情影响，2020年初在线教育、网络支付等大部分网络应用的用户规模呈现较大幅度增长。在此积极发展背景下，却存在不法分子利用疫情期间从事窃取用户隐私信息、传播不法内容、实施疫情相关诈骗的不法行径，对大众的信息安全及财产安全造成威胁。疫情发生期间，360手机卫士积极响应工信部等机关单位号召，站好疫情期间不法信息治理工作的“第一班岗”。根据各类不法信息传播动向实施监控与拦截，遏制其传播态势，结合“疫情工具箱”等产品与防骗宣传，帮助大众了解疫情发展态势的同时，解读当下高发诈骗的实施手法，提高大众的疫情防控与安全防骗意识。

疫情发生以来，各地司法机关强化针对疫情防控期间各类涉疫情犯罪的打击，360手机卫士作为移动安全领域领先的安全类软件，在配合公安机关进行专项打击工作上也积极发挥着自身的技术优势。依靠应龙平台数据关联能力，对涉诈类网址、应用和短信进行关联和溯源分析，从而协助公安进行案件的研判和落地，有效打击涉诈产业链。

《2020年上半年度安全报告》结合上半年度各维度数据及新冠肺炎疫情期间反诈骗数据，联合中国信息通信研究院对目前移动安全发展趋势与黑灰产业相关产业链进行研究分析。文章中突出上半年度网络安全行业动态、360手机卫士作为移动安全领域领先的安全类软件所承担的社会责任、呼吁全行业提高电信网络诈骗防范与黑灰产业治理策略等。

面对当前复杂而严峻的网络安全形势，360将持续运营产生安全能力，“做新时代的网络安全运营商”为明确定位，持续抵制互联网不法信息传播，维护用户移动信息安全。

摘要

恶意程序

- 2020年上半年度，360安全大脑共截获移动端新增恶意程序样本约104.8万个，平均每天截获新增手机恶意程序样本约0.6万个。新增恶意程序类型主要为资费消耗，占比82.0%；其次为隐私窃取（13.6%）、恶意扣费（2.3%）、流氓行为（1.6%）、远程控制（0.4%）与欺诈软件（0.1%）。
- 2020年上半年度，在360安全大脑的支撑下，360手机卫士累计为全国手机用户拦截恶意程序攻击约19.8亿次，平均每天拦截手机恶意程序攻击约1089.8万次。
- 从省级分布来看，2020年上半年度遭受手机恶意程序攻击最多的地区为河南省，占全国拦截量的8.2%；其次为山东（8.2%）、广东（7.8%）、江苏（6.7%）、河北（6.3%）等。
- 从城市分布来看，2020年上半年度遭受手机恶意程序攻击最多的城市为重庆市，占全国拦截量的2.1%；其次为北京（2.0%）、成都（1.6%）、上海（1.5%）、广州（1.3%）等。

钓鱼网站

- 2020年上半年度，360安全大脑在PC端与移动端共为全国用户拦截钓鱼网站攻击约435.8亿次，PC端拦截量约为429.1亿次，占总拦截量的98.5%，平均每日拦截量约2.4亿次；移动端拦截量约为6.7亿次，占总拦截量的1.5%，平均每日拦截量约369.6万次。
- 2020年上半年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达65.9%；其次为假药（13.4%）、虚假购物（11.1%）、金融证券（3.2%）、虚假中奖（3.1%）、网站被黑（1.8%）、模仿登陆（0.5%）、假冒银行（0.5%）、彩票预测（0.3%）与虚假招聘（0.2%）。
- 2020年上半年度，360安全大脑共截获各类新增钓鱼网站2416.3万个，平均每天新增13.3万个。观察钓鱼网站新增类型，境外彩票类占据首位，占比39.5%；其次为金融证券类，占比39.2%。
- 从省级分布来看，2020年上半年度度移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的21.3%；其次为山东（9.8%）、广西（8.0%）、四川（5.7%）、北京（4.6%）等。
- 从城市分布来看，2020年上半年度移动端拦截钓鱼网站最多的城市为北京市，占全国拦截量的4.4%；其次为广州（2.9%）、石家庄（2.5%）、上海（2.3%）、深圳（1.9%）等。

骚扰电话

- 2020年上半年度，360安全大脑收获用户主动标记各类骚扰号码（包括360手机卫士自动检出的响一声电话）约837.3万个，平均每天标记约4.6万个。结合360安全大脑骚扰电话基础数据，360手机卫士共为全国用户识别和拦截各类骚扰电话约98.3亿次，平均每天识别和拦截骚扰电话约0.5亿次。

- 从骚扰电话标记类型来看，响一声以63.3%的比例位居首位；其次为广告推销（11.8%）、骚扰电话（8.6%）、疑似欺诈（6.4%）、房产中介（4.5%）、保险理财（3.7%）、招聘猎头（1.6%）与诈骗电话（0.2%）。
- 从骚扰电话拦截类型来看，骚扰电话以61.1%的比例位居首位；其次为广告推销（22.9%）、疑似欺诈（9.3%）、房产中介（5.1%）、保险理财（0.8%）、响一声（0.4%）、招聘猎头（0.4%）与教育培训（0.1%）。
- 2020年上半年度，从骚扰电话拦截号码个数分布看，被拦截运营商为中国移动的个人手机号最多，占比高达32.4%；其次为固话（24.2%）、运营商为中国联通的个人手机号（22.7%）、运营商为中国电信的个人手机号（16.4%）、虚拟运营商（3.6%）与95/96开头号段（0.7%）。
- 从省级分布来看，2020年上半年度广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的11.8%；其次是山东（7.1%）、江苏（6.8%）、北京（5.3%）、四川（5.1%）等。
- 从城市分布来看，2020年上半年度北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的5.3%；其次是上海（4.5%）、广州（3.5%）、深圳（2.0%）、天津（1.8%）等。
- 从省级分布来看， 2020年上半年度广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的11.3%；其次是山东（7.7%）、江苏（5.9%）、河南（5.7%）、四川（5.2%）等。
- 从城市分布来看，2020年上半年度北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的3.4%；其次是上海（3.2%）、广州（2.8%）、重庆（2.1%）、成都（2.0%）等。

垃圾短信

- 2020年上半年度，在360安全大脑的支撑下，360手机卫士共为全国用户拦截各类垃圾短信约74.9亿条，平均每日拦截垃圾短信约4116.1万条。
- 2020年上半年度，垃圾短信的类型分布中广告推销短信最多，占比为94.8%；诈骗短信占比5.1%；违法短信占比0.1%。
- 从诈骗短信拦截类型来看，诈骗短信以65.9%的比例位居首位；其次为赌博诈骗（25.5%）、兼职诈骗（2.4%）、已识别诈骗号码所发送的诈骗短信（2.0%）、冒充银行（1.9%）、短信内容中预留联系方式涉嫌诈骗（1.1%）与股票诈骗（1.0%）等。
- 从违法短信拦截类型来看，违法金融信贷短信以87.4%的比例位居首位；其次为疑似伪基站发送（7.2%）、售卖信息（2.6%）、恶意催债（1.5%）与色情短信（0.1%）等。
- 2020年上半年度，短信平台106开头号段依然是传播垃圾短信的主要号源，占比高达86.4%。
- 除短信平台1065/1069号段发送垃圾短信外，从其他发送者号码个数分布看，利用虚拟运营商发送垃圾短信的最多，占比34.5%；其次是运营商为中国电信的个人手机号（26.5%）、运营商为中国联通的个人手机号（18.4%）、95/96号段（12.9%）、运营商为中国移动的个人手机号（6.4%）、固话（0.8%）与14物联网卡（0.5%）等。

- 从省级分布来看，2020年上半年度广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的17.2%；其次是山东（8.4%）、浙江（6.2%）、江苏（6.2%）、河南（5.7%）等。
- 从城市分布来看，2020年上半年度广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的8.1%；其次是北京（5.9%）、深圳（4.2%）、上海（3.3%）、南京（3.0%）等。

网络诈骗

- 2020年上半年度360手机先赔共接到手机诈骗举报1561起。其中诈骗申请为776起，涉案总金额高达778.9万元，人均损失10037元。
- 在所有诈骗申请中，金融理财占比最高，为26.7%；其次是虚假兼职（18.2%）、赌博博彩（12.0%）、交友（11.5%）、身份冒充（9.9%）、虚假购物（7.6%）等。
- 从涉案总金额来看，同样是金融理财类诈骗总金额最高，达272.4万元，占比35.0%；其次是身份冒充诈骗，涉案总金额193.4万元，占比24.8%；赌博博彩排第三，涉案总金额为135.1万元，占比17.3%。
- 2020年上半年度，手机诈骗中身份冒充、赌博博彩、金融理财属于高危诈骗类型；虚假兼职属于中危诈骗类型。其中，身份冒充类人均损失最高，约2.5万元；赌博博彩类人均损失约为1.5万元；　其次为金融理财类，人均损失约为1.3万元。
- 从举报用户的性别差异来看，男性受害者占58.8%，女性占41.2%，男性受害者占比高于女性。从人均损失来看，男性为8929元，女性为11616元。
- 从被骗网民的年龄段上看，90后的手机诈骗受害者占所有受害者总数的38.1%；其次是00后占比为28.9%；80后占比为22.3%；70后占比为7.3%、60后占比为2.8%等。
- 从用户举报情况来看，2020年上半年度广东（11.3%）、山东（7.1%）、河南（6.6%）、四川（5.5%）、湖北（5.4%）这5个地区的被骗用户最多。
- 从用户举报情况来看，2020年上半年度上海（2.3%）、深圳（2.2%）、广州（1.9%）、北京（1.7%）、天津（1.5%）这5个城市的被骗用户最多。

关键词：恶意程序、钓鱼网站、骚扰电话、垃圾短信、网络诈骗

目录

第一章 恶意程序 ……7
一. 恶意程序新增样本量与类型分布……7
二. 恶意程序拦截量……8
三. 恶意程序发展趋势分析……8
四. 恶意程序拦截量地域分……9
第二章 钓鱼网站……11
一. 移动端钓鱼网站拦截占……1
二. 移动端钓鱼网站各月拦截量分布 ……11
三. 移动端钓鱼网站类型分布 ……12
四. 移动端钓鱼网站新增 ……12
五. 移动端钓鱼网站拦截量地域分布 ……13
第三章 骚扰电话……15
一. 骚扰电话标记数与拦截量 ……15
二. 骚扰电话标记与拦截类型分布 ……16
三. 骚扰电话拦截号码号源分布 ……17
四. 骚扰电话归属地分 ……18
第四章 垃圾短信……21
一. 垃圾短信拦截量 ……21
二. 垃圾短信类型分析……22
三. 垃圾短信发送者运营商号源分布……23
四. 垃圾短信拦截量地域分析……24
第五章 2020年上半年度手机诈骗概况……26
一. 报案数量与类型 ……26
二. 害者性别与年龄 ……27
三. 受害者地域分布 ……29
第六章 疫情期间反诈骗数据概况……31
一. 疫情期间诈骗电话&短信拦截趋势……31
二. 疫情关键词违法&诈骗短信统计……32
三. 疫情相关的关键词覆盖度 ……33
四. 疫情期间违法&诈骗短信影响地域……33
五. 疫情期间诈骗短信内预留非法联系方式统计 ……34
六. 疫情期间相关违法&诈骗短信发送者号段分布……34
第七章 2020年上半年度重点趋势分析 ……36

目录

一. 网络贷款诈骗套路越来越深,已成诈骗重灾区……36
二. 应用封装与分发平台遭利用，成为应用伪装的“加工厂”……41
三. 博彩诈骗产业链研究……46
第八章 2020年上半年度热门“诈骗剧本”……51
一. 兼职挣钱？实为赌博诈骗！……51
二. 网贷被骗数万元，虚假借贷诈骗又见抬头之势……52
三. 女网友裸聊背后的“桃色陷阱”……53
四. 在线破解！冒充网游交易平台实施诈骗全过程……54
五. 刷单再现支付陷阱，“高倍镜”找出破绽！……55
六. “万亿”市值还给原始股，虚拟货币平台背后的“套路”……56
第九章 2020年上半年度网络安全行业动态……59
一. 工信部：做好疫情防控期间信息通信行业网络安全保障工作……59
二. 警惕“95”号段诈骗 层层转包已成产业链……59
三. 犯罪团伙利用“裸聊”敲诈勒索……60
四. 警方捣毁特大跨境“网络赌博”洗钱团伙……61
五. 工信部：纵深推进App侵害用户权益专项整治……62
六. 工信部发布工作方案运用大数据技术防治电信网络诈骗……62
第十章 社会责任……64
一. “安全大脑”助力抗疫反诈工作，配合工信部守护用户移动安全……64
二. 协助公安机关，打击黑灰产业链初见成效……65
三. 关注女性人身安全，发起女性安全公益行动……68
第十一章 提高电信网络诈骗防范与治理策略……71
一. 不断完善技术策略，加强产业链治理打击……71
二. 跨部门多方协作，加强预警封堵措施……71
三. 丰富安全宣传方式，加强反诈安全意识……71

第一章　恶意程序

移动终端作为移动互联网的重要组成部分，正持续遭受着恶意程序的侵扰。互联网技术持续发展的同时，恶意程序的“更新换代”也同样在进行。不法分子逃避监管的手段愈加繁复，伪装手段也愈加“花样”，可实现在人们无感知情况下，进行隐私窃取或财产盗刷。

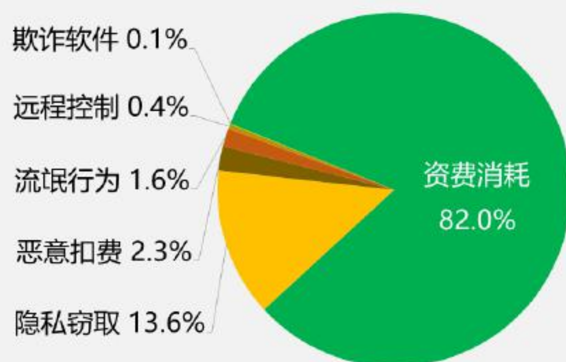
2020年上半年，受疫情因素影响人们利用移动设备的使用时长增加，也无形中增加了“中招”几率。不法分子正是利用这一敏感时段，大肆传播恶意程序，实现获利。其中恶意程序类型以资费消耗类为主，色情视频类APP为主要“工具”。为有效防护移动互联网安全，360安全大脑持续加强对移动互联网恶意程序的识别和拦截力度，以保障移动互联网健康的有序发展。

一.恶意程序新增样本量与类型分布

2020年上半年度，360安全大脑共截获移动端新增恶意程序样本约104.8万个，同比2019年上半年度（92.0万个）上升了12.2%，平均每天截获新增手机恶意程序样本约0.6万个。下图为2020年上半年度移动端各月新增恶意程序样本量统计：

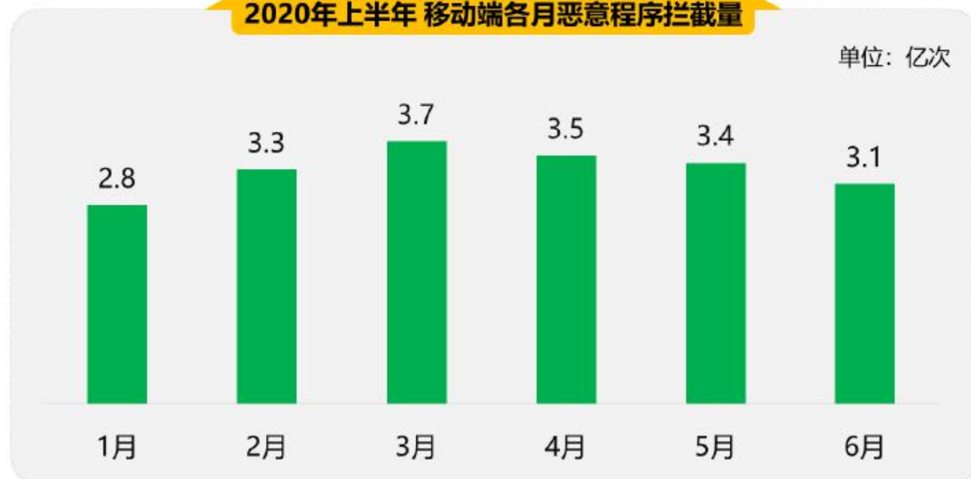


2020年上半年度，移动端新增恶意程序类型主要为资费消耗，占比82.0%；其次为隐私窃取（13.6%）、恶意扣费（2.3%）、流氓行为（1.6%）、远程控制（0.4%）与欺诈软件（0.1%）。下图为2020年上半年度移动端新增恶意程序类型分布：



二.恶意程序拦截量

2020年上半年度，在360安全大脑的支撑下，360手机卫士累计为全国手机用户拦截恶意程序攻击约19.8亿次，平均每天拦截手机恶意程序攻击约1089.8万次。下图为2020年上半年度移动端各月恶意程序



三.恶意程序发展趋势分析

2019年第四季度至2020年上半年期间，恶意程序新增量在2019年12月出现激增峰值，当月恶意程序新增量为31.6万。自2020年1月起，恶意程序新增持续呈现持续下降趋势，恢复以往平均新增值。但在2020年4月份，恶意程序再次出现新增峰值，当月恶意程序新增量为29.2万。根据趋势预测，恶意程序作为不法分子的典型“作案工具”，新增恶意程序走高已成为主要趋势。

反观恶意程序拦截量趋势，直线上涨走势明显，在2020年第二季度呈现降低走势。拦截量突增主要体现在2020年第一季度。第一季度中，新增恶意程序个数减少，但遭受恶意程序侵害的现象频发。由于第一季度受到春节假期前后与疫情影响，大众日常使用网络时长增加，无形中提高了遭受网络不法信息侵害的几率。不法分子利用这一敏感时间段，大肆传播恶意程序，实现不良获利。

2020年上半年度恶意程序TOP排行，色情视频类APP传播范围较广，且APP数量众多。存在恶意消耗用户资费与窃取用户隐私数据的恶意应用较多。



四.恶意程序拦截量地域分布

2020年上半年度，从省级分布来看，遭受手机恶意程序攻击最多的地区为河南省，占全国拦截量的8.2%；其次为山东（8.2%）、广东（7.8%）、江苏（6.7%）、河北（6.3%），此外、四川、浙江、安徽、湖南、广西的恶意程序拦截量也排在前列。



从城市分布来看，遭受手机恶意程序攻击最多的城市为重庆市，占全国拦截量的2.1%；其次为北京（2.0%）、成都（1.6%）、上海（1.5%）、广州（1.3%），此外石家庄、郑州、深圳、西安、天津的恶意程序拦截量也排在前列。



第二章 钓鱼网站

随着移动设备数量的不断增长，针对移动设备的钓鱼网站攻击也愈加明显。排除有明显恶意行为的典型钓鱼网站，金融借贷类钓鱼网站同样具有高风险，用户易遭到信息泄露、高利贷款，甚至贷款诈骗等风险。网络借贷具备申请便利、下款快等特征，近几年受到大众的追捧。网络借贷的火热，吸引了众多“鱼龙混杂”的借贷平台上线。受疫情影响，金融借贷诈骗案件持续高发，已成为受害人数最多、涉案金额最高的诈骗类型。

针对金融借贷发展现状，360安全大脑及时调整相关拦截策略，针对金融借贷类钓鱼网站建立研究专项，大大提升了样本检测量与样本拦截能力，在用户遭遇欺诈前，及时识别疑似包含恶意行为的金融借贷类网站，以防护用户的信息安全与财产安全。

一.移动端钓鱼网站拦截占比

2020年上半年度，360安全大脑在PC端与移动端共为全国用户拦截钓鱼网站攻击约435.8亿次，同比2019年上半年度（404.2亿次）上升了7.3%。其中，PC端拦截量约为429.1亿次，占总拦截量的98.5%，平均每日拦截量约2.4亿次；移动端拦截量约为6.7亿次，占总拦截量的1.5%，平均每日拦截量约369.6万次。下图为2020年上半年度钓鱼网站拦截占比分布：



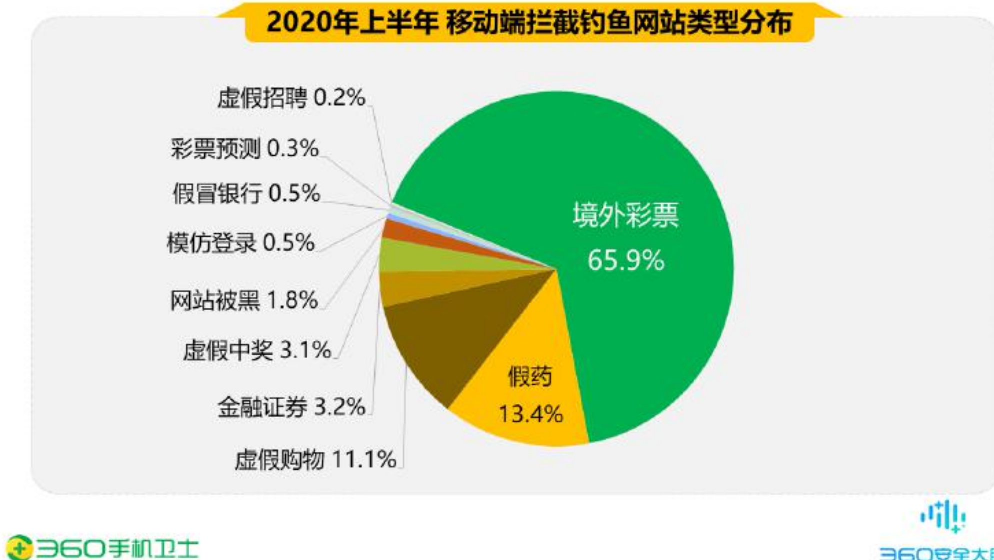
二.移动端钓鱼网站各月拦截量分布

2020年上半年度，360安全大脑在移动端拦截钓鱼网站攻击约为6.7亿次，同比2019年上半年度（13.8亿次）下降51.1%。下图为2020年上半年度钓鱼网站各月拦截量分布：



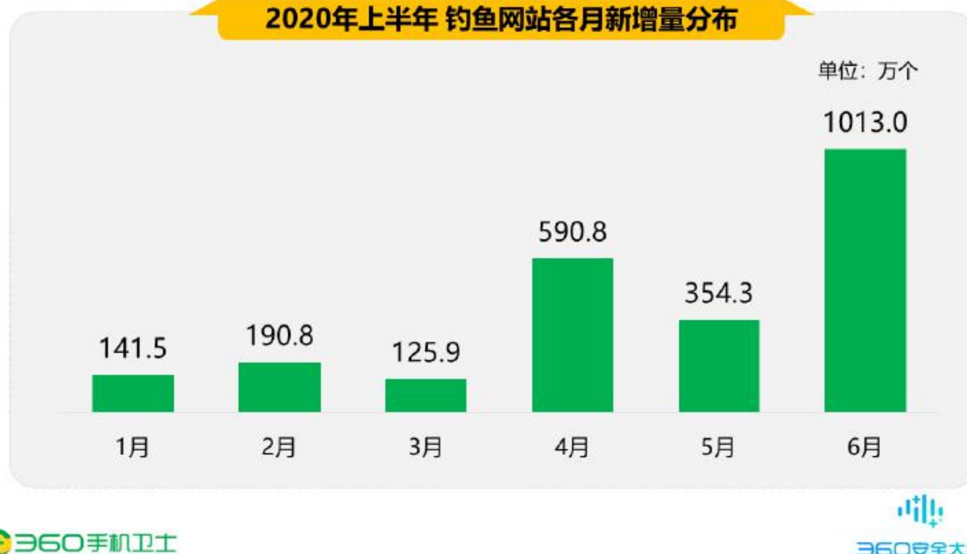
三.移动端钓鱼网站类型分布

2020年上半年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达65.9%；其次为假药（13.4%）、虚假购物（11.1%）、金融证券（3.2%）、虚假中奖（3.1%）、网站被黑（1.8%）、模仿登陆（0.5%）、假冒银行（0.5%）、彩票预测（0.3%）与虚假招聘（0.2%）。下图为2020年上半年度移动端拦截钓鱼网站类型分布：



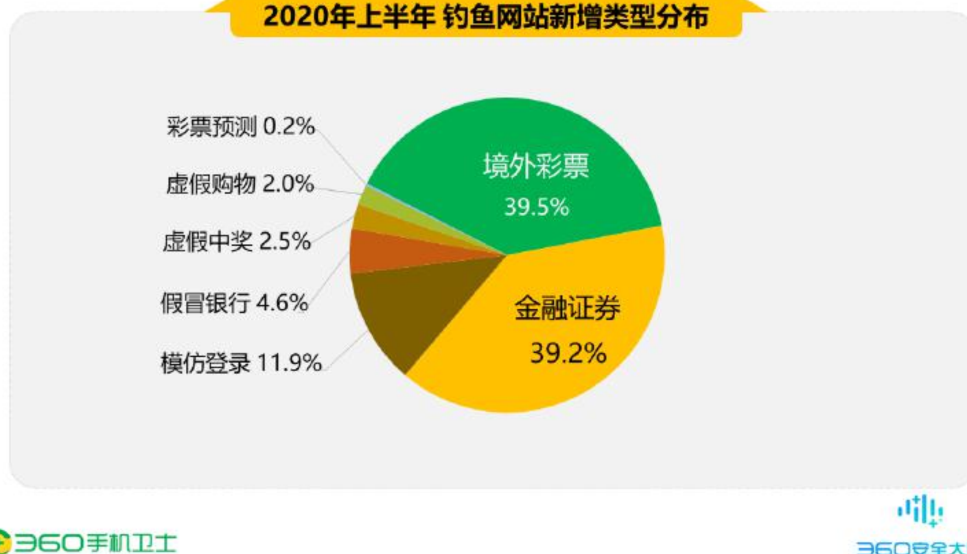
四.移动端钓鱼网站新增量

2020年上半年度，360安全大脑共截获各类新增钓鱼网站2416.3万个，同比2019年上半年度（1019.2万个）上升了57.8%，平均每天新增13.3万个。



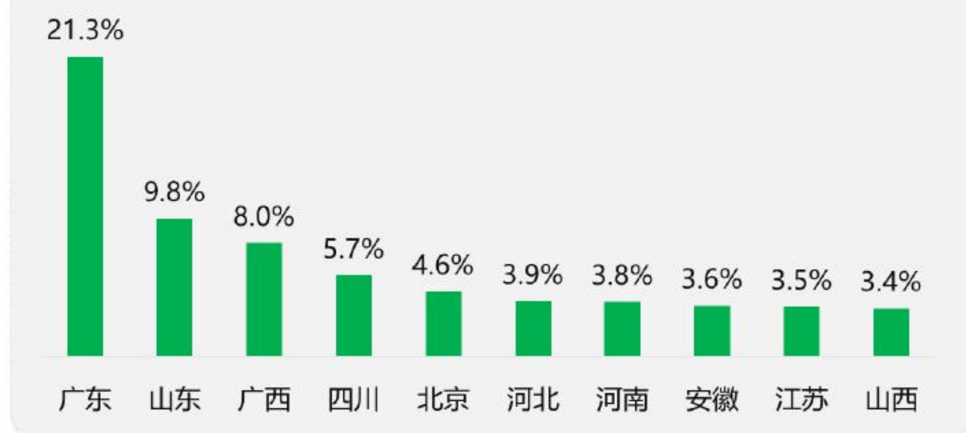
观察钓鱼网站新增类型，境外彩票类占据首位，占比39.5%；其次为金融证券类，占比39.2%。

随着近几年网络贷款的兴起，互联网中贷款平台丛生，资质参差不齐，滋生了大量虚假贷款平台。第一季度受疫情原因影响，部分大众收入来源遭受影响，由于网络贷款具备快捷、便利、下款快的特点，很多人选择利用网络贷款缓解经济压力，不法分子便利用此社会现象大肆传播虚假贷款平台，导致贷款诈骗案件频发。针对这一现状，360安全大脑及时调整相关拦截策略，针对金融借贷类钓鱼网站建立研究专项，大大提升了样本检测量与样本拦截能力，在用户遭遇欺诈前，及时识别疑似包含恶意行为的金融借贷类网站，以防护用户的信息安全与财产安全。

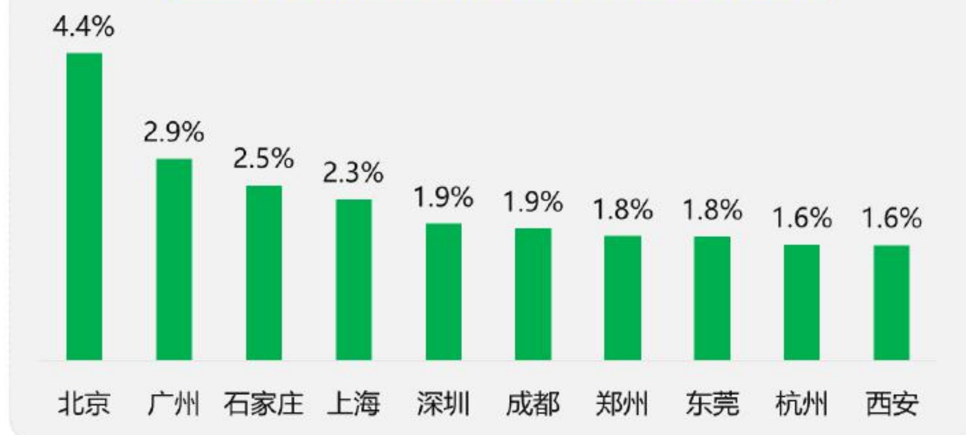


五.移动端钓鱼网站拦截量地域分布

2020年上半年度，从省级分布来看，移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的21.3%；其次为山东（9.8%）、广西（8.0%）、四川（5.7%）、北京（4.6%），此外河北、河南、安徽、江苏、山西的钓鱼网站拦截量也排在前列。



从城市分布来看，移动端拦截钓鱼网站最多的城市为北京市，占全国拦截量的4.4%；其次为广州（2.9%）、石家庄（2.5%）、上海（2.3%）、深圳（1.9%），此外成都、郑州、东莞、杭州、西安的钓鱼网站拦截量也排在前列。



第三章 骚扰电话

骚扰电话一直具备利用特定时段进行传播的特征，在2020年第一季度疫情爆发时期，骚扰电话的传播似乎并没有受到疫情影响，依旧呈现高发态势。通过骚扰电话发展趋势可见，疫情期间在陌生电话呼入整体数量下降的同时，360手机卫士针对骚扰电话的识别和拦截比例则呈现逐步上升的态势。

骚扰电话发展趋势依旧严峻。通信技术的成熟发展为拨打骚扰电话提供了成本更低、呼入更高效的渠道及方式。当前不法分子利用虚拟号段与95/96号段实施电信诈骗的案件时有发生，已成为不法分子传播利用的新渠道。骚扰电话背后极具规模的灰色产业链在各环节的紧密衔接下形成闭环，并相互推动。秉承《综合整治骚扰电话专项行动方案》，360安全大脑利用自身大数据、人工智能等技术手段协助治理骚扰电话乱象，重点整治商业营销类、恶意骚扰类和违法犯罪类骚扰电话。

一.骚扰电话标记数与拦截量

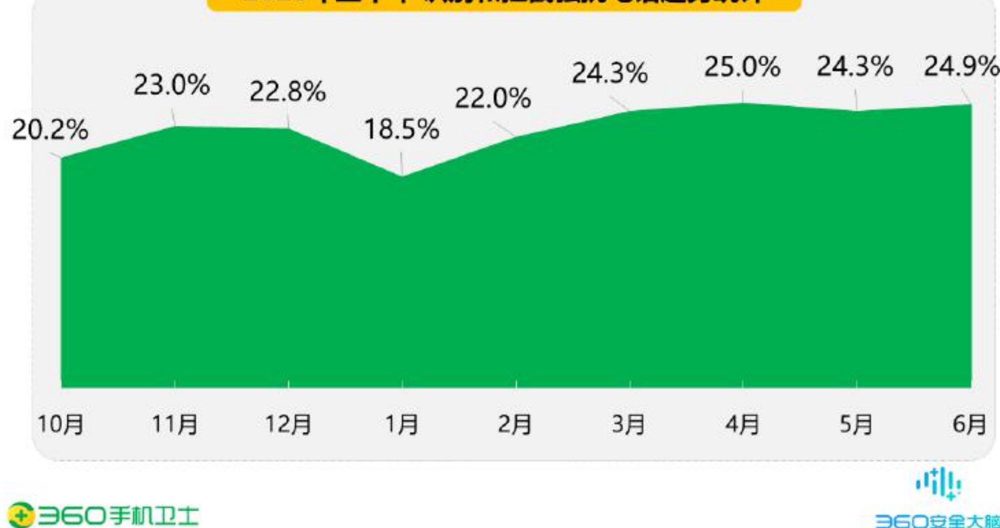
2020年上半年度，360安全大脑收获用户主动标记各类骚扰号码（包括360手机卫士自动检出的响一声电话）约837.3万个，平均每天标记约4.6万个。从标记号码个数上看，同比2019年上半年度（3800.6万个）下降了77.9%。下图为2020年上半年度骚扰电话各月标记号码个数分布：



结合360安全大脑骚扰电话基础数据，360手机卫士共为全国用户识别和拦截各类骚扰电话约98.3亿次，平均每天识别和拦截骚扰电话约0.5亿次。同比2019年上半年度（112.8亿次）下降了12.9%。下图为2020年上半年度骚扰电话各月拦截号码次数分布：

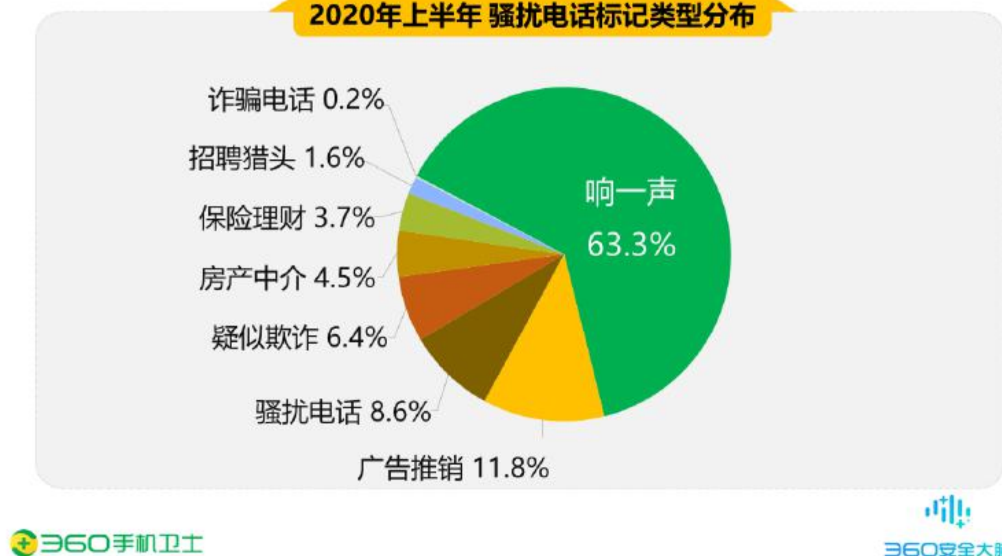


根据各月骚扰电话呼入占比分析，2020年1月份临近春节假期，骚扰电话拦截量最低。在春节前后，从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低，与往年趋势一致。但自2020年2月份起，在陌生来电整体呼入量下降的情况下，骚扰电话比例却处于逐步上升的现象，且发展趋势逐步走高，说明不法分子从事电信骚扰并未受到疫情因素影响，疑似利用疫情这一敏感时段，从事不法信息的传播与骚扰。下图为2020年上半年识别与拦截骚扰电话趋势统计：

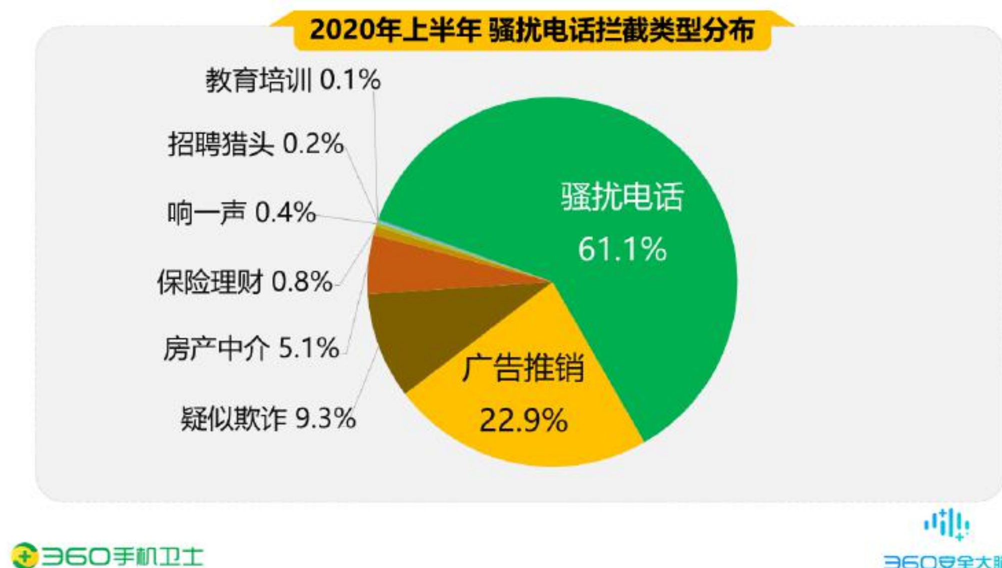


二.骚扰电话标记与拦截类型分布

2020年上半年度，综合360安全大脑的拦截监测情况及用户调研分析，从骚扰电话标记类型来看，响一声以63.3%的比例位居首位；其次为广告推销（11.8%）、骚扰电话（8.6%）、疑似欺诈（6.4%）、房产中介（4.5%）、保险理财（3.7%）、招聘猎头（1.6%）与诈骗电话（0.2%）。下图为2020年上半年度骚扰电话标记类型分布：

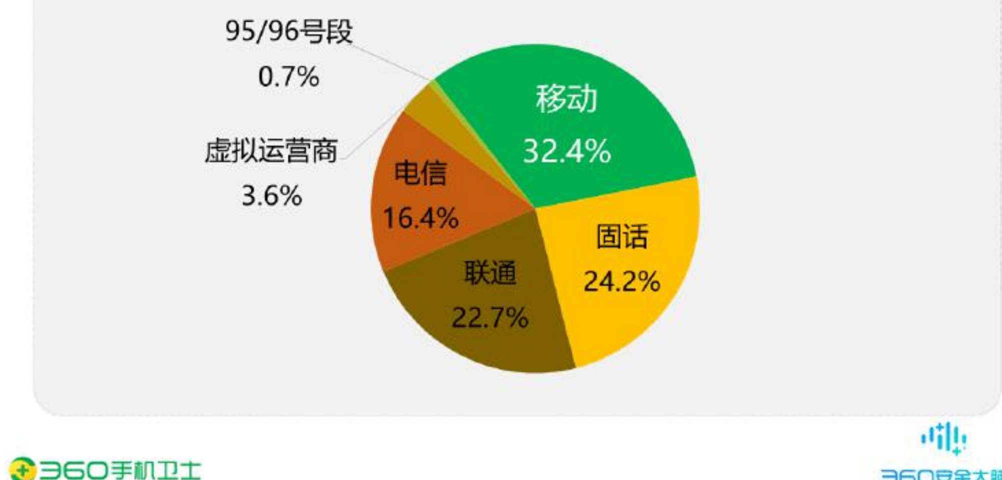


从骚扰电话拦截类型来看，骚扰电话以61.1%的比例位居首位；其次为广告推销（22.9%）、疑似欺诈（9.3%）、房产中介（5.1%）、保险理财（0.8%）、响一声（0.4%）、招聘猎头（0.4%）与教育培训（0.1%）。下图为2020年上半年度骚扰电话拦截类型分布：

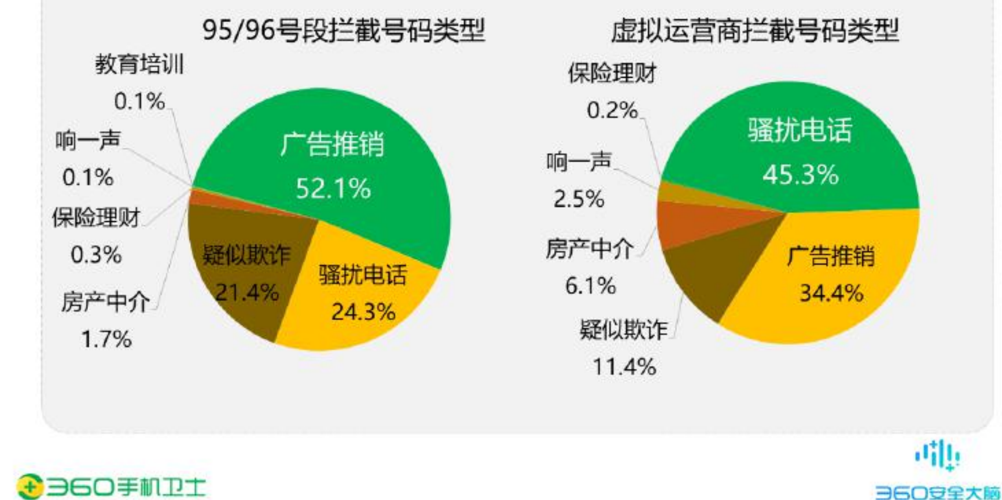


三.骚扰电话拦截号码号源分布

2020年上半年度，从骚扰电话拦截号码个数分布看，被拦截运营商为中国移动的个人手机号最多，占比高达32.4%；其次为固话（24.2%）、运营商为中国联通的个人手机号（22.7%）、运营商为中国电信的个人手机号（16.4%）、虚拟运营商（3.6%）与95/96开头号段（0.7%）。下图为2020年上半年骚扰电话拦截号码号源分布：



观察95/96号段与虚拟运营商骚扰电话拦截号码类型，95/96号段广告推销类占据首位，占比52.1%；虚拟运营商骚扰电话类占据首位，占比45.3%；疑似欺诈类分别占比21.4%与11.4%，类型比例占据前列。95/96号段与虚拟运营商号码遭不法分子利用，是不法分子从事非法行径的主要“工具”之一。

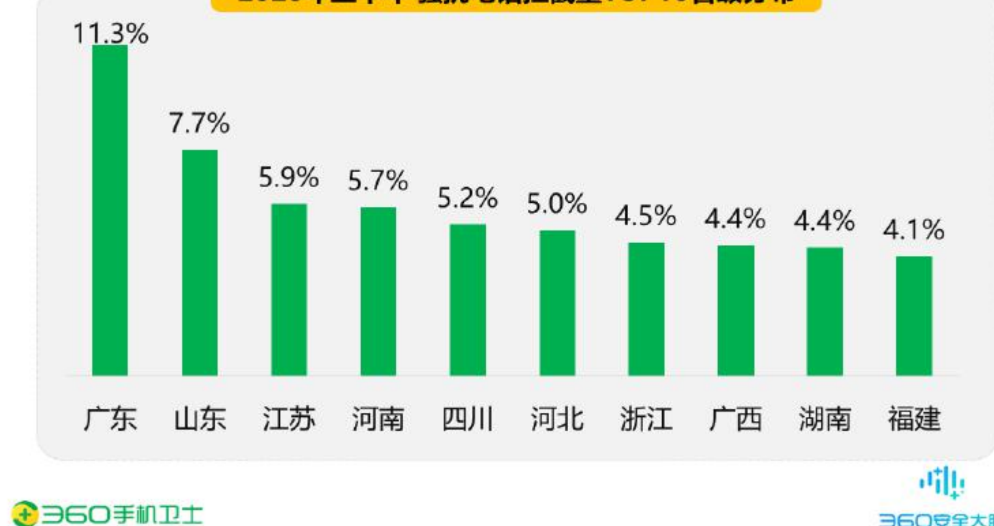


四.骚扰电话归属地分布

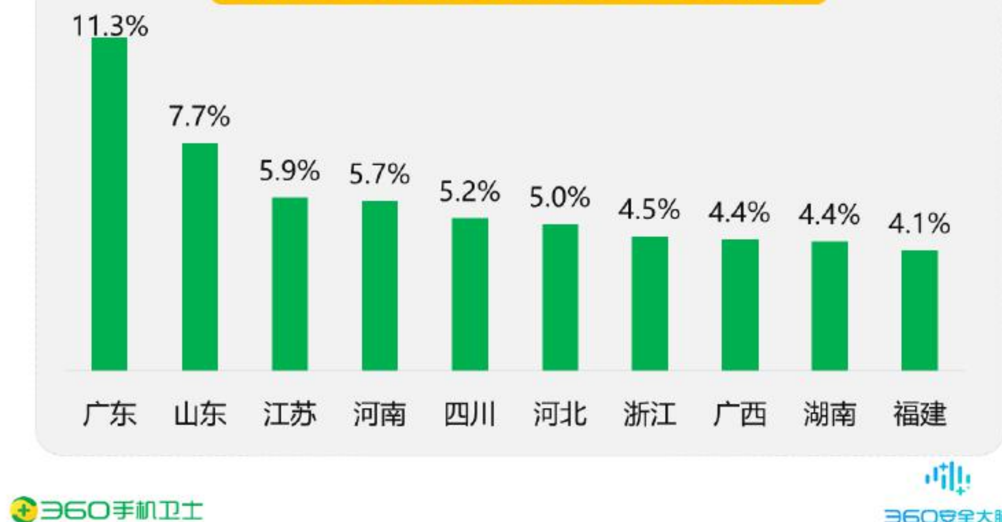
2020年上半年度，从各地骚扰电话标记号码个数上分析，广东省用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的11.8%；其次是山东（7.1%）、江苏（6.8%）、北京（5.3%）、四川（5.1%），此外河南、上海、浙江、河北、湖南的骚扰电话标记号码个数也排在前列。



从城市分布来看，北京市用户标记骚扰电话号码的个数最多，占全国骚扰电话标记号码个数的5.3%；其次是上海（4.5%）、广州（3.5%）、深圳（2.0%）、天津（1.8%），此外杭州、重庆、苏州、南京、西安的骚扰电话标记号码个数也排在前列。



2020年上半年度，从各地骚扰电话的拦截量上分析，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的11.3%；其次是山东（7.7%）、江苏（5.9%）、河南（5.7%）、四川（5.2%），此外河北、浙江、广西、湖南、福建的骚扰电话拦截量也排在前列。



从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的3.4%；其次是上海（3.2%）、广州（2.8%）、重庆（2.1%）、成都（2.0%），此外深圳、天津、东莞、苏州、郑州的骚扰电话拦截量也排在前列。



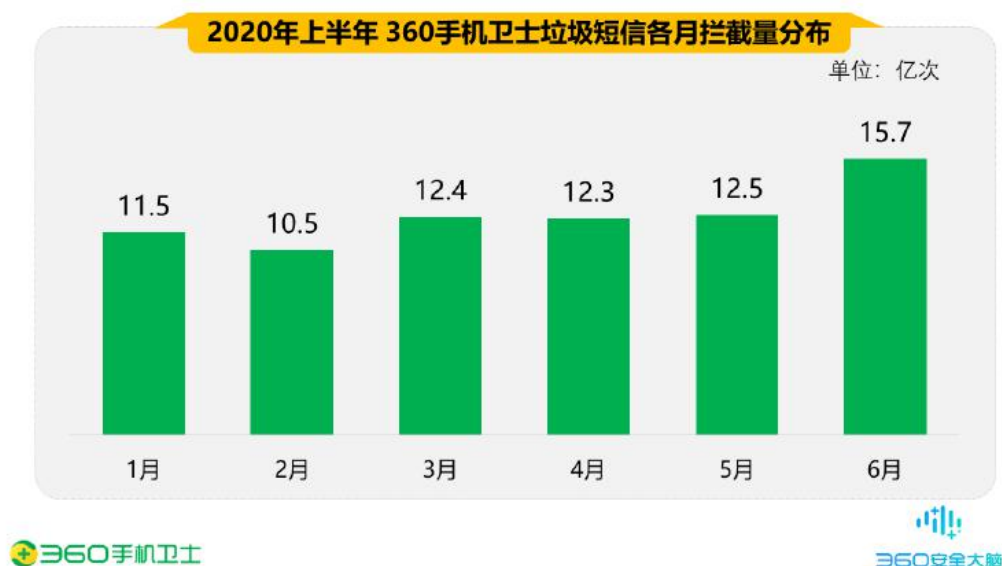
第四章 垃圾短信

近几年，垃圾短信所带来的危害越来越引起了社会各界的广泛重视，随着运营商、手机厂商、安全厂商等对垃圾短信的管控打击，其发展趋势得以遏制。但随着通信技术的发达，短信平台、虚拟号段与95/96号段成为不法分子传播违法诈骗短信的新一级渠道，并在短信内容中利用关键词、变体字等实现“攻防”，帮助不法内容进行传播。

当前短信平台、虚拟号段与95/96号段传播不法内容的现状，360安全大脑已于云端建立相关拦截规则，并提升本地算法能力，实时研判垃圾短信传播中的新增与变种，帮助用户抵制垃圾短信所带来的骚扰与侵害。

一.垃圾短信拦截量

2020年上半年度，在360安全大脑的支撑下，360手机卫士共为全国用户拦截各类垃圾短信约74.9亿条，同比2019年上半年度（23.3亿条）上升了68.8%，平均每日拦截垃圾短信约4116.1万条。下图为2020年上半年度360手机卫士垃圾短信各月拦截量分布：

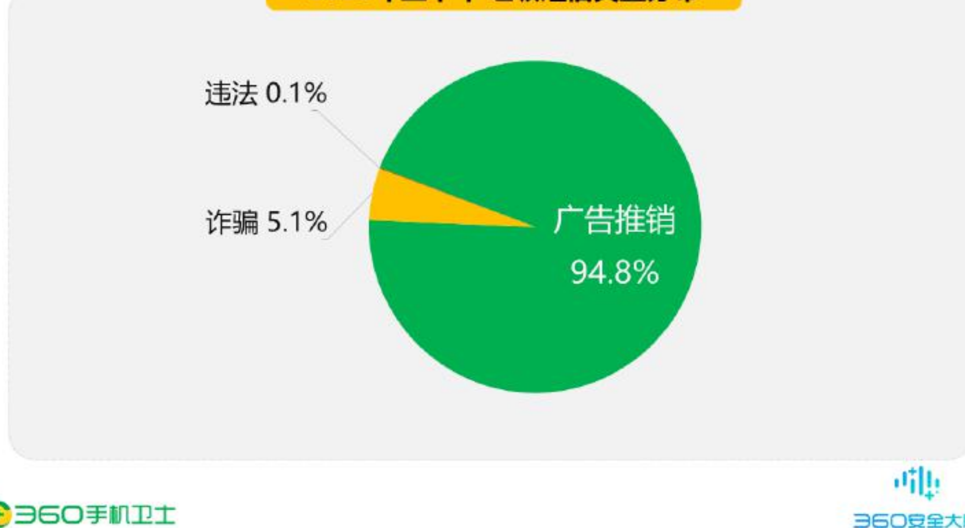


根据垃圾短信拦截量趋势分布，2019年Q4季度呈现涨幅态势。根据往年趋势，年底一般为垃圾短信传播高峰期，并随着春节假期的临近而逐渐回落。同时由于疫情影响，2020年2月份垃圾短信拦截量持续降低，在3月份复工复产后，垃圾短信拦截量逐渐回升，并呈现持续走高态势。6月份出现2020年上半年垃圾短信拦截量峰值，当月拦截量为15.7亿次。

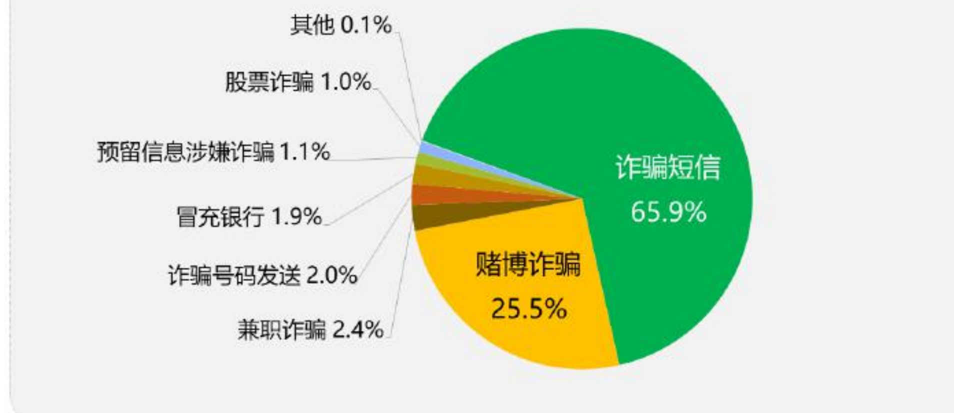


二.垃圾短信类型分析

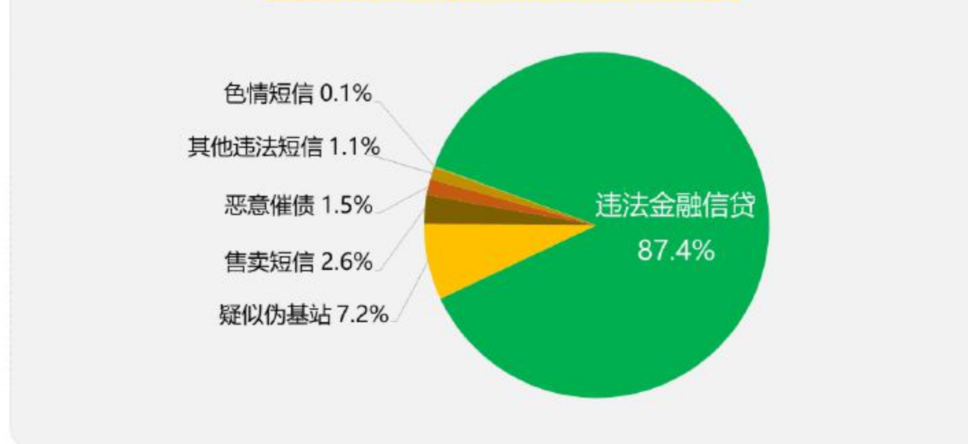
2020年上半年度，垃圾短信的类型分布中广告推销短信最多，占比为94.8%；诈骗短信占比5.1%；违法短信占比0.1%。



从诈骗短信拦截类型来看，诈骗短信以65.9%的比例位居首位；其次为赌博诈骗（25.5%）、兼职诈骗（2.4%）、已识别诈骗号码所发送的诈骗短信（2.0%）、冒充银行（1.9%）、短信内容中预留联系方式涉嫌诈骗（1.1%）与股票诈骗（1.0%）等。下图为2020年上半年度诈骗短信子类型分布：

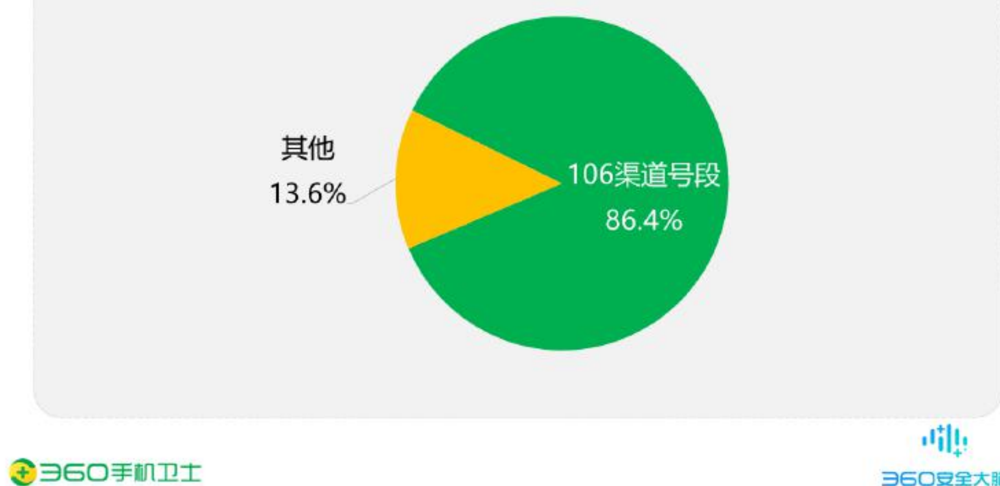


从违法短信拦截类型来看，违法金融信贷短信以87.4%的比例位居首位；其次为疑似伪基站发送（7.2%）、售卖信息（2.6%）、恶意催债（1.5%）与色情短信（0.1%）等。下图为2020年上半年度违法短信子类型分布：

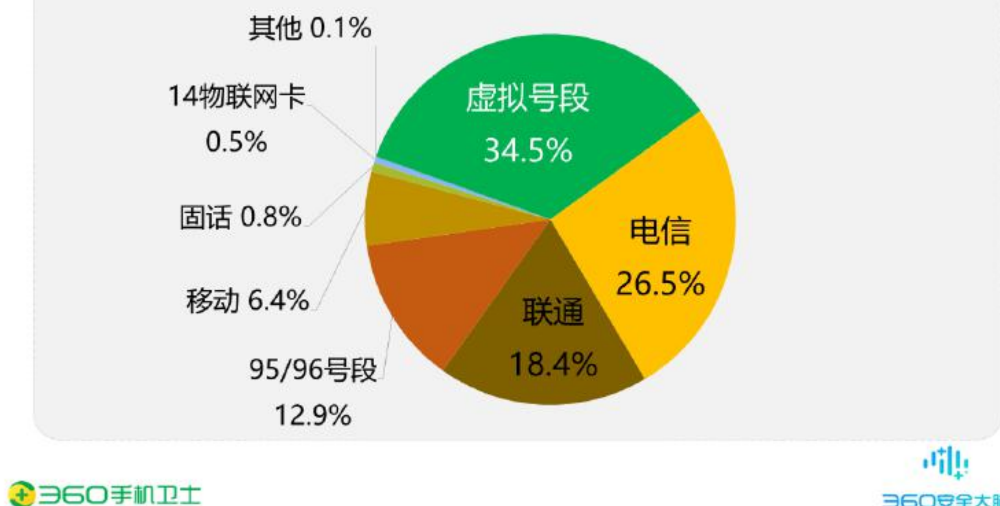


三.垃圾短信发送者运营商号源分布

2020年上半年度，短信平台106开头号段依然是传播垃圾短信的主要号源，占比高达86.4%；利用其他号段传播垃圾短信占比约13.6%。利用短信平台、虚拟运营商传播各类型短信，已成为目前主流趋势。从获取用户联系方式到群发短信，已形成完整产业链条。与此同时，其发送成本低、传播范围广的特点被黑灰产业利用，成为传播违法诈骗类短信的重要渠道。虽然当前针对短信平台传播垃圾短信的现状已有相关部门与安全厂商实现联合打击治理，但目前发展现状却依然严峻，短信平台与虚拟运营商号段是当下垃圾短信治理的重要方向。下图为2020年上半年度短信平台发送垃圾短信占比分布：



2020年上半年度，除短信平台106开头号段发送垃圾短信外，从其他发送者号码个数分布看，利用虚拟运营商发送垃圾短信的最多，占比34.5%；其次是运营商为中国电信的个人手机号（26.5%）、运营商为中国联通的个人手机号（18.4%）、95/96号段（12.9%）、运营商为中国移动的个人手机号（6.4%）、固话（0.8%）与14物联网卡（0.5%）等。



四.垃圾短信拦截量地域分析

2020年上半年度，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的17.2%；其次是山东（8.4%）、浙江（6.2%）、江苏（6.2%）、河南（5.7%），此外河北、北京、四川、湖南、山西的垃圾短信拦截量也排在前列。



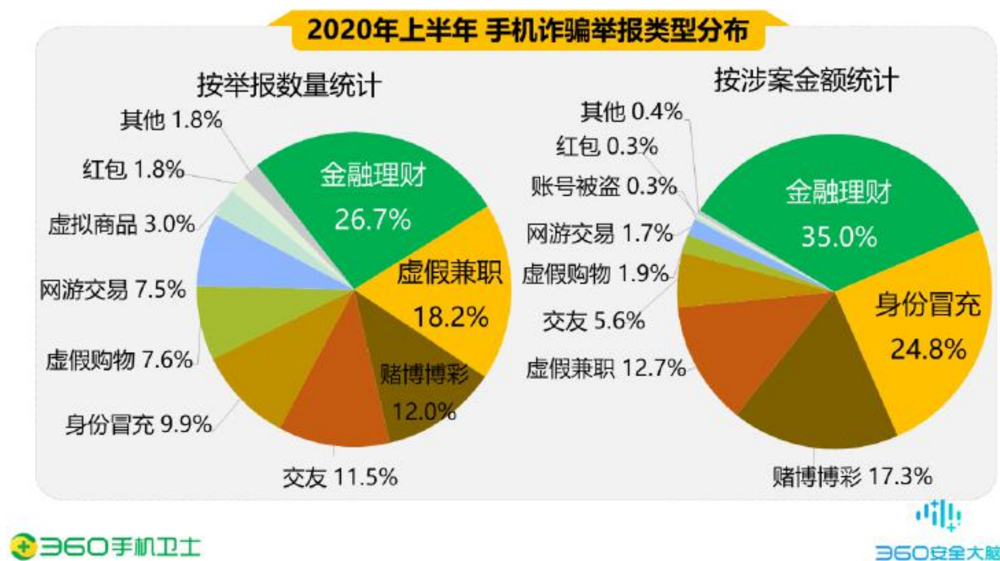
从城市分布来看，广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的8.1%；其次是北京（5.9%）、深圳（4.2%）、上海（3.3%）、南京（3.0%），此外重庆、杭州、石家庄、成都、西安的垃圾短信拦截量也排在前列。



第五章 2020年上半年度手机诈骗概况

一.报案数量与类型

2020年上半年度360手机先赔共接到手机诈骗举报1561起。其中诈骗申请776起，涉案总金额高达778.9万元，人均损失10037元。在所有诈骗申请中，金融理财占比最高，为26.7%；其次是虚假兼职（18.2%）、赌博博彩（12.0%）、交友（11.5%）、身份冒充（9.9%）、虚假购物（7.6%）等。从涉案总金额来看，同样是金融理财类诈骗总金额最高，达272.4万元，占比35.0%；其次是身份冒充诈骗，涉案总金额193.4万元，占比24.8%；赌博博彩排第三，涉案总金额为135.1万元，占比17.3%。下图为2020年上半年度手机诈骗类型的举报类型与涉案金额分布情况：



2020年上半年度，手机诈骗中身份冒充、赌博博彩、金融理财属于高危诈骗类型；虚假兼职属于中危诈骗类型。其中，身份冒充类人均损失最高，约2.5万元；赌博博彩类人均损失约为1.5万元；其次为金融理财类，人均损失约为1.3万元。

（1）2020年上半年度中身份冒充类主要以冒充亲友与冒充客服为主，其次为冒充公检法。其中，冒充亲友主要为伪装身份向通讯录好友借钱、伪装亲友出事讨要费用；冒充客服人员主要为冒充官方平台客服，以订单异常、快递丢失、商品质量存在问题需退款等借口实施诈骗，诱导用户进行转账；另外，在2020年在疫情期间，存在不法分子冒充公检法机关人员，利用疫情期间受害人护照被扣留、存在不明出境记录、社保卡涉嫌骗保等借口实施诈骗的案例发生，且涉案金额巨大。

(2)赌博博彩类一直属于手机诈骗中的高发类型，在2020年第一季度疫情期间尤为突出，半年度也依然处于诈骗TOP前三。其手法主要以事前 “赠送彩金”为吸引点，诱导用户在赌博网站

充值赌资，后期限制提现导致用户损失；或以“赚钱”为噱头引导至赌博平台进行兼职操作，例如

刷单、彩票跟投等，但后期不返还本金与佣金。随着移动端用户群体的激增，赌博博彩跟随潮流，呈现出PC端向移动端倾斜发展的现状。诈骗实施中，不法分子引导用户通过移动端设备访问赌博网站或下载APP充值赌资成为主流手段。由于第一季度疫情的出现，用户居家隔离且缺少社交娱乐活动及赚钱方式，因此利用网络寻找消遣及赚钱成为多数用户的选择，不法分子在此期间“推波助澜”，借助互联网渠道大肆宣传赌博平台，导致赌博博彩类案例频发，人均损失高达1.5万元。

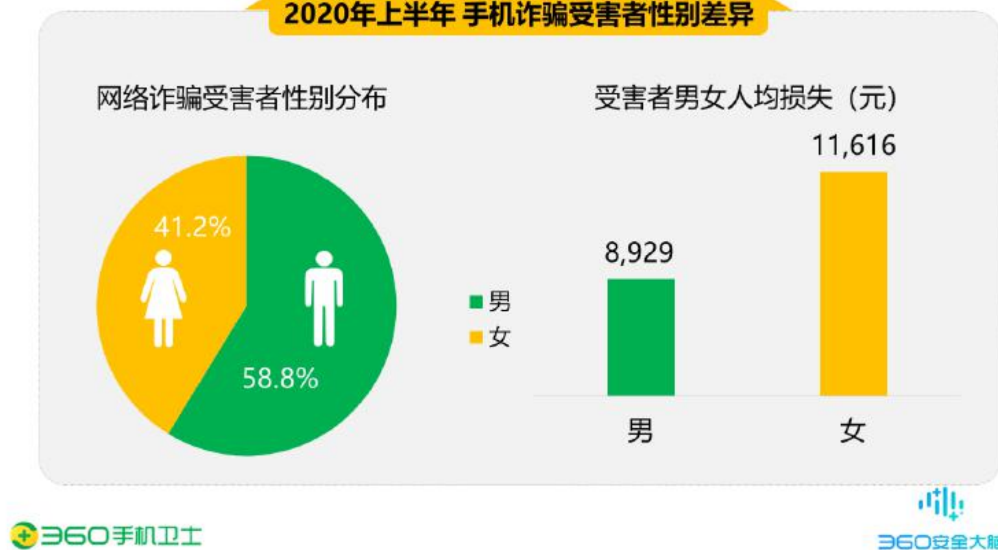
(3)2020年上半年度中金融理财类是受骗人数最多且涉案损失最高的类型，主要体现为网络贷款被骗。收取贷款手续费、包装费或引导用户下载借贷APP操作属于借贷诈骗的主要手法。同样受到疫情影响，大多数人选择利用网络贷款缓解经济压力。一般来说网络中无抵押贷款、秒下款等借贷广告更易吸引眼球，在双方成功取得联系后，不法分子将会通过多种方式要求用户进行付款操作。超前消费已成为普遍社会现象，贷款诈骗正是利用这一社会痛点实现疯狂蔓延，目前依然呈现高发态势。贷款诈骗案例中，首次与用户联系时，通过电话方式与用户沟通的现象较多，但通过上半年度金融理财案例的汇总，通过社交平台实施贷款诈骗的比例上升，疑似成为宣传并实施贷款诈骗的新兴渠道。

(4)2020年上半年度虚假兼职类型以兼职缴纳会费的手法居多。受到疫情影响，尝试通过网络赚钱缓解经济压力成为部分人的选择之一。由于不法分子通常利用社交平台发布兼职广告，吸引众多用户进行兼职任务，在此敏感时间段，更是打着疫情的旗号，招揽更多用户参与，导致遭受诈骗的用户数量居高不下。

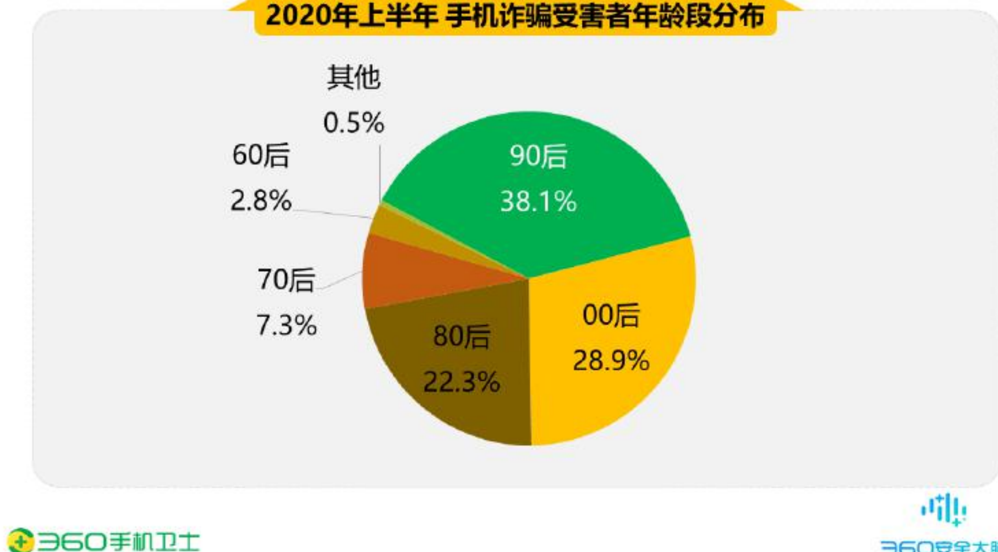


二.受害者性别与年龄

2020年上半年度，从举报用户的性别差异来看，男性受害者占58.8%，女性占41.2%，男性受害者占比高于女性。从人均损失来看，男性为8929元，女性为11616元，女性人均损失高于男性。下图为2020年上半年手机诈骗受害者性别差异：



从被骗网民的年龄段上看，90后的手机诈骗受害者占所有受害者总数的38.1%，是不法分子从事网络诈骗的主要受众人群；其次是00后，占比为28.9%；80后占比为22.3%；70后占比为7.3%、60后占比为2.8%等。下图为2020年上半年手机诈骗受害者年龄段分布：

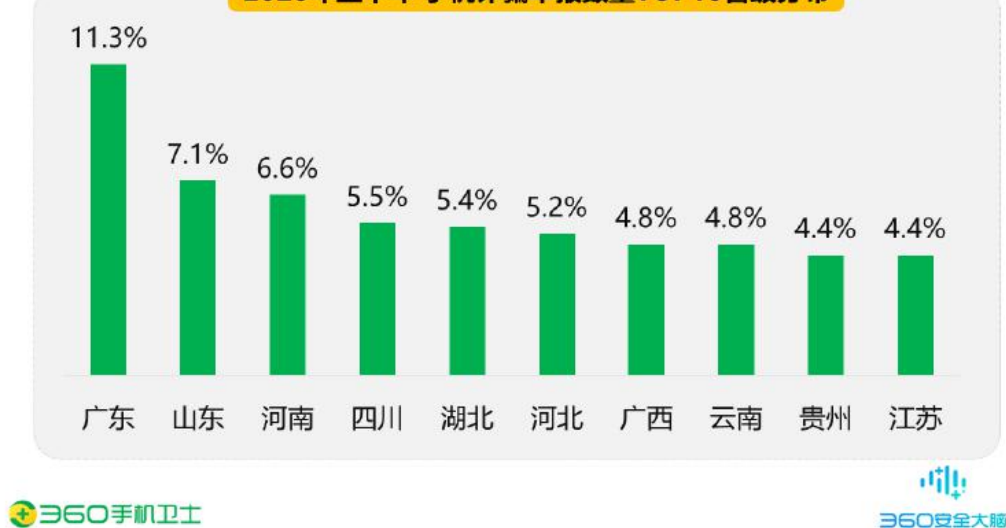


2020年上半年度，00后与90后受骗人数较为接近。但是通过对比发现，00后被骗的人数虽多，但由于这个年龄段用户经济能力有限，被骗平均金额相对较少。90后作为2020年上半年度诈骗主要针对人群，人均损失也较高。80后及以上年龄段日常使用网络的时间有限，遭受诈骗的人数也较少。但由于这部分用户有一定经济实力，在遭受诈骗时，损失金额也相对较高。



三.受害者地域分布

2020年上半年度，从各地区手机诈骗的举报情况来看，广东（11.3%）、山东（7.1%）、河南（6.6%）、四川（5.5%）、湖北（5.4%）这5个地区的被骗用户最多，举报数量约占到了全国用户举报总量的36.0%。下图给出了2020年上半年度手机诈骗举报数量最多的10个省份：



从各城市手机诈骗的举报情况来看，上海（2.3%）、深圳（2.2%）、广州（1.9%）、北京（1.7%）、天津（1.5%）这5个城市的被骗用户最多，举报数量约占到了全国用户举报总量的9.7%。下图给出了2020年第一季度手机诈骗举报数量最多的10个城市：


2020年上半年 手机诈骗举报数量TOP10城市分布
2.3%
2.2%
1.9%
1.7%
1.5%
1.5%
1.5%
1.3%
1.3%
1.3%
上海
深圳
广州
北京
天津
东莞
武汉
青岛
昆明
重庆
360手机卫士
360安全大脑

第六章 疫情期间反诈骗数据概况

一.疫情期间诈骗电话&短信拦截趋势

2020年上半年度，疫情防控作为重点工作的同时，针对诈骗电话与诈骗短信传播不良信息的治理工作也在同步进行。2020年1月份诈骗电话拦截量最高，平均每日拦截量约为802万次；2月份拦截数量出现骤降，诈骗电话平均每日拦截量约为360万次，环比1月份每日拦截量下降55.1%；后续数据显示截至6月30日，疫情发生期间诈骗电话发展处于平缓下降趋势。

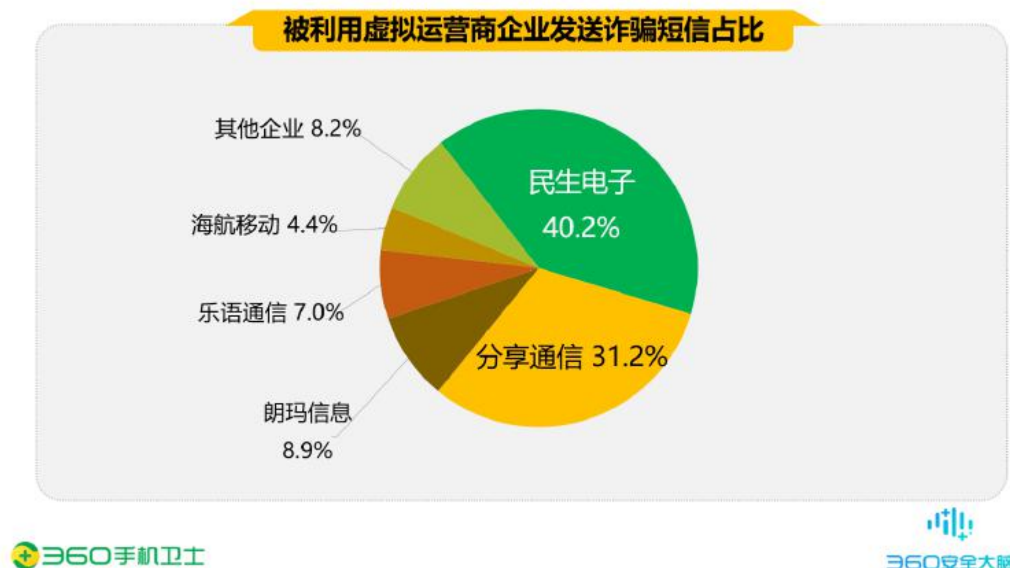


2020年第一季度，属于疫情防控的重要时期。观察第一季度数据，1月份诈骗短信平均每日拦截量约为270万条，在1月底的疫情爆发初期呈现下降趋势，但后续呈现逐日上涨趋势，并在2月9日出现诈骗短信拦截量峰值，约为580万条。自2月10日起，又继续呈现下降趋势并逐渐趋于平稳。2月份，诈骗短信平均每日拦截量约为348万条，环比1月份每日拦截量上升28.7%。截至6月30日，疫情发生期间诈骗短信发展同样处于平缓下降趋势。



由图可见，1月份底正值春节假期，从事诈骗活动的人员减少，导致诈骗电话与短信的拦截量骤减。在2月初，诈骗电话拦截量出现小幅回升，诈骗短信数量则呈现激增趋势。该现象产生的原因在于此时间疫情防控工作陆续开展，民众对于疫情防护的关注度提高，不法分子利用这一特殊的时间节点，从事各类涉及疫情的诈骗行动。如：售卖口罩、口罩资金盘、疫情兼职、贷款等。由于后期政府、媒体等渠道对各类诈骗事件进行了公开曝光，并予以打击，因而有效的提高了大众的防骗意识。在2020年第二季度，全国疫情局势已得到遏制，2月下旬至6月底，诈骗电话与短信的拦截量趋于平缓发展并呈现明显降低态势。

2月份是疫情防控工作开展的重要时段，诈骗短信在此时段内呈现激增态势，其中包括借助疫情期间传播的诈骗短信。根据诈骗短信的发送者号段统计，利用虚拟运营商号段传播非法内容的占比较高。抽取2月份上旬虚拟运营商号段所发送的诈骗短信，对被不法分子利用传播不法内容的虚拟运营商企业进行统计显示，其中民生电子占比40.2%；其次为分享通信（31.2%）、朗玛信息（8.9%）、乐语通信（7.0%）、海航移动（4.4%）等。



简称	公司全称
民生电子	民生电子商务有限责任公司
分享通信	北京分享在线网络技术有限公司
朗玛信息	贵阳朗玛信息技术股份有限公司
乐语通信	北京乐语通信科技有限公司
海航移动	海南海航信息技术有限公司

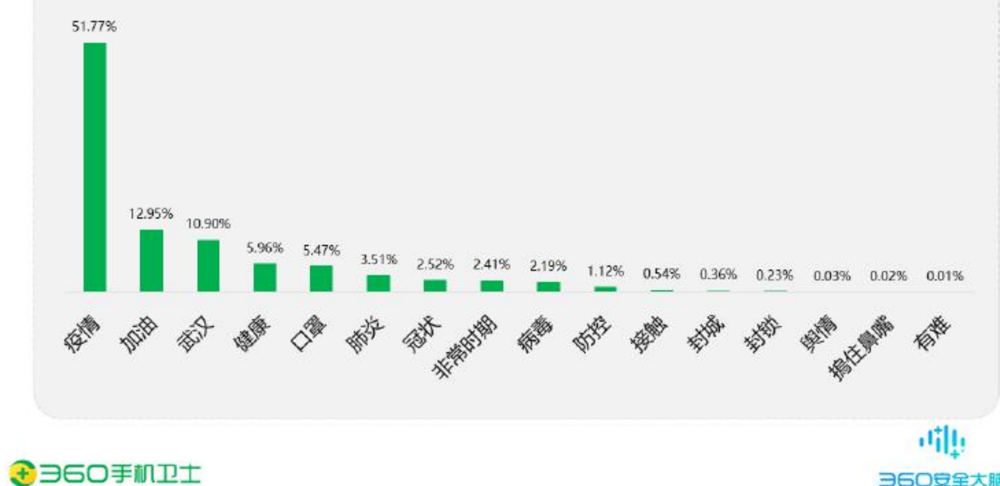
二.疫情关键词违法&诈骗短信统计

疫情期间（0124-0526）短信内容中包含与疫情的关键词并判定属于违法&诈骗短信的，共拦截约54.3万条，平均每日拦截量约为4377条。



三.疫情相关的关键词覆盖度

随机抽取（0205-0212）短信进行关键词覆盖度统计，其中与疫情相关的关键词“疫情”占比最高，占比51.77%；其次为“加油”（12.95%）、“武汉”（10.90%）。详细关键词占比统计如下：



四.疫情期间违法&诈骗短信影响地域

疫情期间（0203-0526），通过各地域与疫情相关的违法&诈骗短信拦截量统计，用户接收违法&诈骗短信最多的是广东省，占全国与疫情相关违法&诈骗短信拦截量的15.3%；其次为四川（8.9%）、山东（5.9%）、浙江（5.6%）、河南（5.3%），湖南、广西、河北、江苏、江西与疫情相关的违法&诈骗短信拦截量也排在前列。



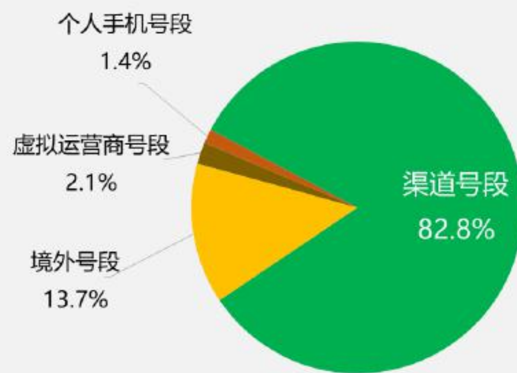
五.疫情期间诈骗短信内预留非法联系方式统计

疫情期间，抽取2月份诈骗短信进行短信内预留非法联系方式进行统计，其中拦截QQ共计4820次，占比2.0%；微信9768次，占比4.0%；URL231517条，占比94.1%；抽取短信中，赌博类诈骗短信占近9成，其他类型包括兼职诈骗、涉政类违法短信。预留非法联系方式去重后显示，QQ725个，微信账号729个，URL5264条。



六.疫情期间相关违法&诈骗短信发送者号段分布

疫情期间相关违法&诈骗短信发送者通过运营商号段区分，TOP5号段分别为：渠道号段占比82.8%；其次为境外号段（13.7%）、虚拟运营商号段（2.1%）、个人手机号段（1.4%）。


短信发送者号段占比（包含疫情相关关键词TOP号段）
个人手机号段
1.4%
虚拟运营商号段
2.1%
境外号段
13.7%
渠道号段
82.8%
360手机卫士
360安全大脑

第七章 2020年上半年度重点趋势分析

一.网络贷款诈骗套路越来越深,已成诈骗重灾区

中国经济产业的转型升级让中国金融产品及消费借贷应用得到普及，并由此衍生出了无需物质抵押，依托个人消费记录的电商消费类借贷产品，以及无需物质抵押，依托个人征信的小额借贷产品。但是随着金融市场借贷习惯的养成，在用户体量不断增多的同时，大量的网贷欺诈事件也时有发生，包括高额砍头息的“714高炮”、冒充知名借贷平台的虚假平台等一系列新骗局新手段，也给网络借贷诈骗的打击防范带来了全新的挑战。

于此同时，伴随着互联网行业从PC互联网时代发展到移动互联网时代，黑灰产业也从PC互联网时代的“单兵”作战向移动互联网时代的“集团化”作战转变。随着黑灰产行业的“集团”化和人员分工的“链接”化，其网络安全技术和攻防策略不断演进升级。一方面不断提升欺诈环境的仿真度，防止被用户识别；一方面借助攻防策略的升级来躲避网络安全、社交软件等产品对欺诈样本的识别。鉴于此攻防对抗将是互联网行业与黑灰产“企业”不断厮杀成长的一场持久战。以下通过传播渠道、诈骗应用、实施诈骗三个环节对网络借贷诈骗攻防策略及演变进行解读。

（一）传统渠道之短信内容的攻守之道

随着互联网的发展，从日常沟通到身份验证都离不开短信的身影，手机短信已成为生活中必不可缺的工具。正因如此，黑灰产也时刻紧盯着短信这块传播渠道的“蛋糕”。2020年1月份，诈骗短信平均每日被360拦截量约为270万条（数据来源：360发布的2020年第一季度中国手机安全状况报告）。若按照每人1条短信计算，相当于每日有270万人遭受诈骗短信的“洗礼”，可见诈骗短信的影响程度之深。黑灰产在大量传播欺诈短信的同时，还不断升级短信攻防策略，以应对安全厂商对欺诈短信的识别拦截。

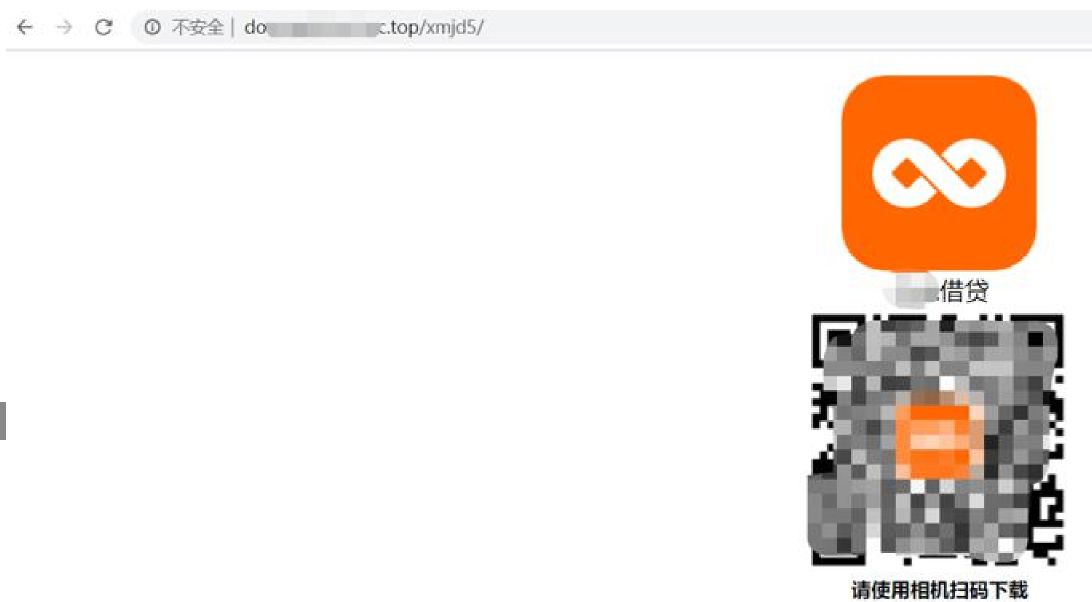
1.短信内容伪造、内容“混淆”

由于传统的网络借贷平台在推广过程中会使用短信进行推广，因此黑灰产常采用冒充知名网络借贷平台的方式传播模仿知名借贷平台短信内容的虚假短信。但随着大数据算法的发展，仅仅通过短信内容模仿已无法突破网络安全厂商的短信识别。于是网络黑灰产开始升级自身短信内容，采用“混淆”短信内容的方式，将短信文字进行简繁体转换并对内容进行语义混淆，如短信内容“【温馨提醒】您友蛛晶卫苓娶 请加Q：(1399***1) w.ur***.cn/***”，这句话潜在含义就是“您有资金未领取”。

2.短信内应用下载链伪装

由于网络安全技术升级迭代，黑灰产采用的混淆短信内容的方式已无法躲避网络安全厂商的算法模式识别，继而网络黑灰产盯上了应用下载链本身。移动浏览器由于设备屏幕大小及用户体验的问题，网址栏一般都会进行隐藏，用户对于访问网站的网址感知度较低，无法通过查看网址信息的方式确认网站真伪。不法分子针对应用的下载链进行“包装”，在页面中增加了对非移动设备的访问限制，迫使访问者使用移动设备的浏览器访问应用下载链。例如通过手机浏览器访问网址时页面会跳出应用的下载链，但通过电脑浏览器访问时，无显示应用下载链，需使用手机扫描指定二维码进行下载，迫使用户使用移动设备访问此网址。


不安全
/xmjd5/
Galaxy S5
360 × 640
100%
浏览器-手机模式
借贷
应用大小：3M
免费安装
安全认证
4.9 ★★★★★
9,999个评分
12+
年龄
1、安卓手机下载完点击安装即可
2、Iphone手机点击安装完返回桌面，如下载完成，则点击设置 >> 通用 >> 企业级应用 >> 点击应用>>信任
简介
评分及评论
4.9
满分 5 分
9,999个评分

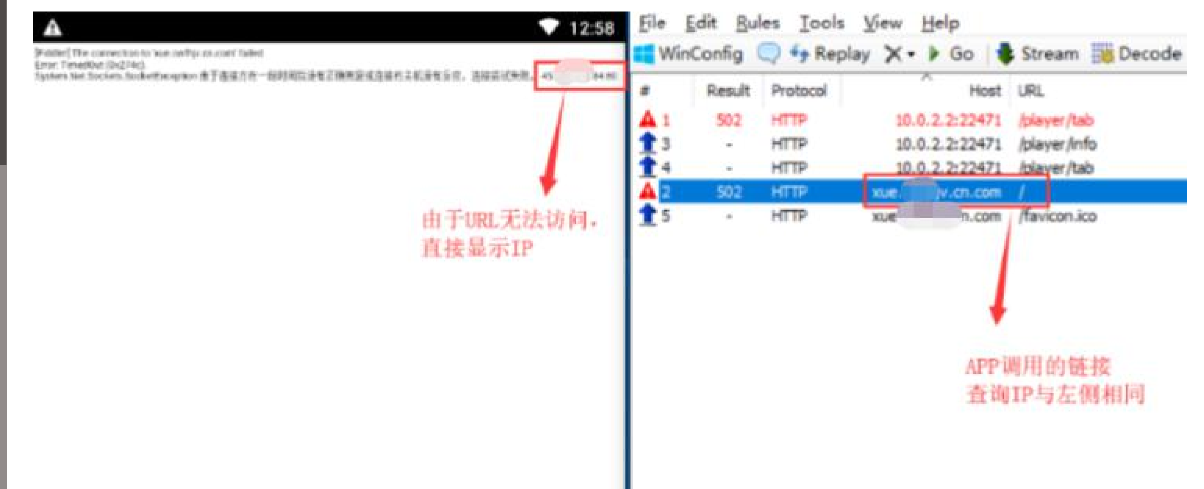

不安全
c.top/xmjd5/
借贷
请使用相机扫码下载

另一方面对虚假应用的真实下载地址进行隐藏。访问者在页面填写验证信息后，才会跳转至应用的下载站。通过这种方式，不法分子一方面获取到了访问者填写的注册信息（手机号、姓名等），一方面防止了应用下载链及安装包轻易被网络安全研究人员获取并分析。但随着网址模型+短信算法模型的升级，此种方式已无法躲避网络安全厂商的“安全大脑”。



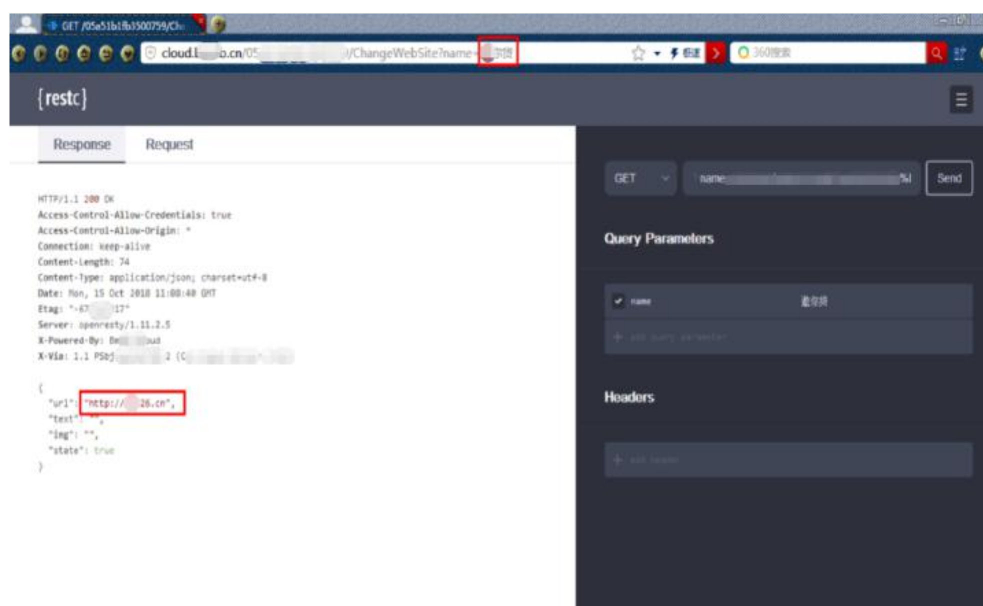
（二）从云控应用与子域名群站

2018年，在对部分虚假借贷应用逆向分析时，发现一部分应用通过网址封装生成，APP显示的内容与网站内容一致。当网站无法访问时，APP也会直接报错。通过下图可看出部分虚假APP调用的网址及报错情况：





在对部分关联的网址深入分析时，发现其通过WEB接口提供商，批量生成不同名称的虚假借贷APP。如“京小贷”APP调用的请求网址为：（http://cloud.b***.cn****=京小贷），不法分子通过更改bm***.cn的链接参数，使得APP调用不同的APP链接。如参数设置为京小贷时，APP调用京小贷的URL，设置为*你贷时，APP调用*你贷的网址。通过查询发现“b***.cn”为一个提供后端服务的平台，为云服务提供商，提供APP源码、数据库、短信验证码等服务。不法分子通过对服务平台的滥用，实现了对虚假借贷APP的批量化生成，使得诈骗类软件的变化更难以控制。



2019年、2020年在对用户举报的虚假贷款应用逆向分析的过程中我们发现，大部分虚假借贷类应用仍通过网址封装生成，但由云控的方式转向通过不同子域名的方式生成不同的网址。如下图展示的应用，其平台使用的网址为36021.****.icu，其子域名36019、36020、36022、36023也为虚假借贷平台。相较于云控方式，子域名形式，其服务器与解析方式可控，不法分子可将子域名解析至不同服务器中的不同web页面，实现单一网站被拦截后快速上线新网站的目的。



云控应用及子域名生成的应用，虽然最终产生的网址不同，但其本质都是调用同一个host域名，一旦判断出该主网站（host）是虚假借贷平台服务时，拦截其主网站（host）其关联的所有虚假贷款即可被识别。

（三）“第三方在线客服平台”代替传统社交软件，或成孵化诈骗的温床

中国互联网的发展推动了在线社交行业的发展，QQ、微信等社交平台由于其便利性、用户群体众多等特点，常被不法分子用于实施诈骗。随着2019年国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室组织开展专项打击行动，对缅北部分电信网络诈骗活动严重区域的QQ、微信、支付宝、POS机等社交和支付账户采取封停措施后，大量诈骗团伙使用的社交账号已遭到停用。

于是不法分子转而将目光盯上了第三方在线客服平台。第三方客服系统类似于CMS（网站内容管理系统），本身是帮助企业解决平台客服接入管理问题。通过平台接口的方式接入企业平台，降低企业研发和运营成本。黑灰产人员利用“虚假”的认证信息，将第三方客服系统接入到虚假贷款平台中，为虚假平台提供在线客服服务。由于是通过接口的方式接入应用中的，诈骗团伙在实施完诈骗关闭虚假贷款平台后，用户与此在线客服平台客服无法进行再次沟通，导致受害人无法保存与骗子沟通的聊天记录，对后期警方的案件侦破造成了一定的困难。

二.应用封装与分发平台遭利用，成为应用伪装的“加工厂”

（一）应用封装与分发平台被黑灰产利用现状

中国移动互联网的快速发展，在造就大量的互联网“人才”的同时，也衍生了众多的互联网业务。而这些业务由于其便利性，逐渐被黑灰产盯上了，成为了黑灰产人员眼中的香饽饽。2020年上半年360手机先赔用户反馈的涉嫌诈骗样本中很多都与封装、分发平台有联系。一部分是借助封装平台进行应用封装，一部分应用是借助分发平台生成应用下载链。借助封装、分发平台的便利，黑灰产人员拥有了批量生成虚假贷款、理财、博彩、交友等类型应用的能力，同时也拥有了应用存储的“安生场所”。不法分子一方面利用仿冒类应用骗取用户的资金。一方面借助恶意类应用获取用户的隐私信息，实施敲诈勒索等诈骗活动。

（二）黑灰产搭建及利用应用封装与分发平台的流程

从互联网诞生起，就建立了源源不断的网站，人们在接触互联网时接触最多的也是网站，可以说网站是搭起整个互联网大旗的“基石”。正因如此，各类网站搭建平台，建站工具迸发。借助各类域名售卖平台、服务器平台、建站CMS迅速搭建出各式各样的网站。随着移动互联网的发展，APP开始进入大众视野，逐渐取代网站成为了时代的新宠儿，但原生开发应用开发难度大，成本高，因此能将网站内容封装成应用的封装平台成为了各类网站站长的“救星”。

通过对涉嫌诈骗的应用分析、应用下载链溯源，发现涉嫌诈骗的应用也利用了封装平台、分发平台的技术。下文通过应用封装、分发的流程，展示部分涉嫌诈骗应用的上线流程。

1.封装平台、分发平台概述：

封装类应用指的是通过分装平台封装出来的应用，封装应用通常由“网站+APP应用客户端”两部分构成。APP封装主要是将对应网站的网址封装在应用内。封装完应用后，打开该APP的过程就是浏览器访问该应用内所封装的网站内容的过程。这种方式与使用浏览器访问网址的效果一样，所以封装的APP大多数也多由网页封装而来。

分发平台指的是应用托管平台，将应用上传至该平台后，由该平台生成应用的下载链。此类平台其主要宣传点是专为内测应用使用，解决应用存储、应用商店审核应用周期长的问题。

2. 封装、分发平台起源及分类

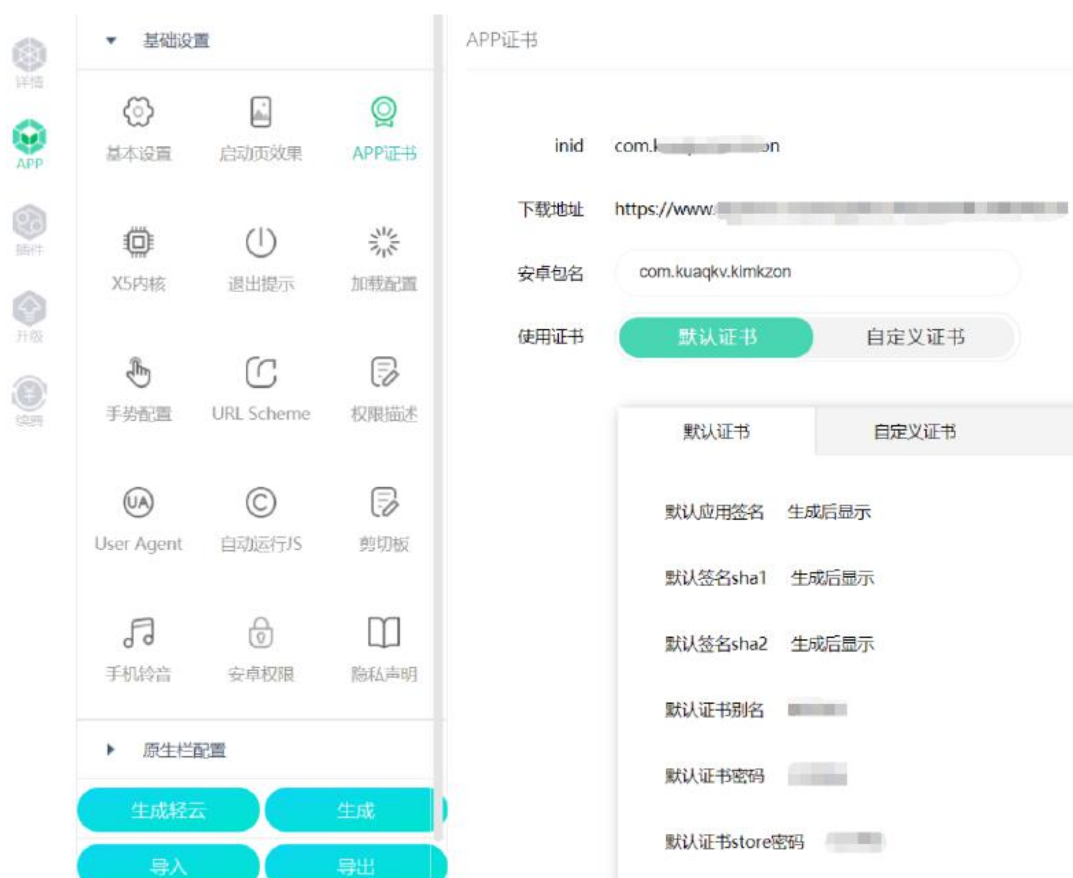
封装平台和分发平台功能联系密切，目前此类服务提供商，会提供封装、分发一站式服务。由于其产业链门槛低，市面上可以发现大量提供应用封装分发的平台，这些平台主打的功能基本都大同小异，主打APP在线封装、分发功能，部分会提供企业签名功能。根据封装平台网站备案信息的不同，运营方的不同。存在企业备案、个人备案、未备案三类平台。网址是企业备案的封装平台，其背后主要是一些科技公司提供技术支撑；网址是个人备案及网址未含有备案信息的封装平台，其主要是个人或者黑灰产从业者，利用一些封装分发平台源码搭建而成。其中封装平台网址中无备案信息的网站，由于其网站的网址未进行域名备案，属于违规网址，所以其主打的功能就是封装应用时，无需使用者在平台进行实名操作。目前由于应用稳定性的问题，黑灰产多使用一些知名度较高的封装平台进行应用封装。

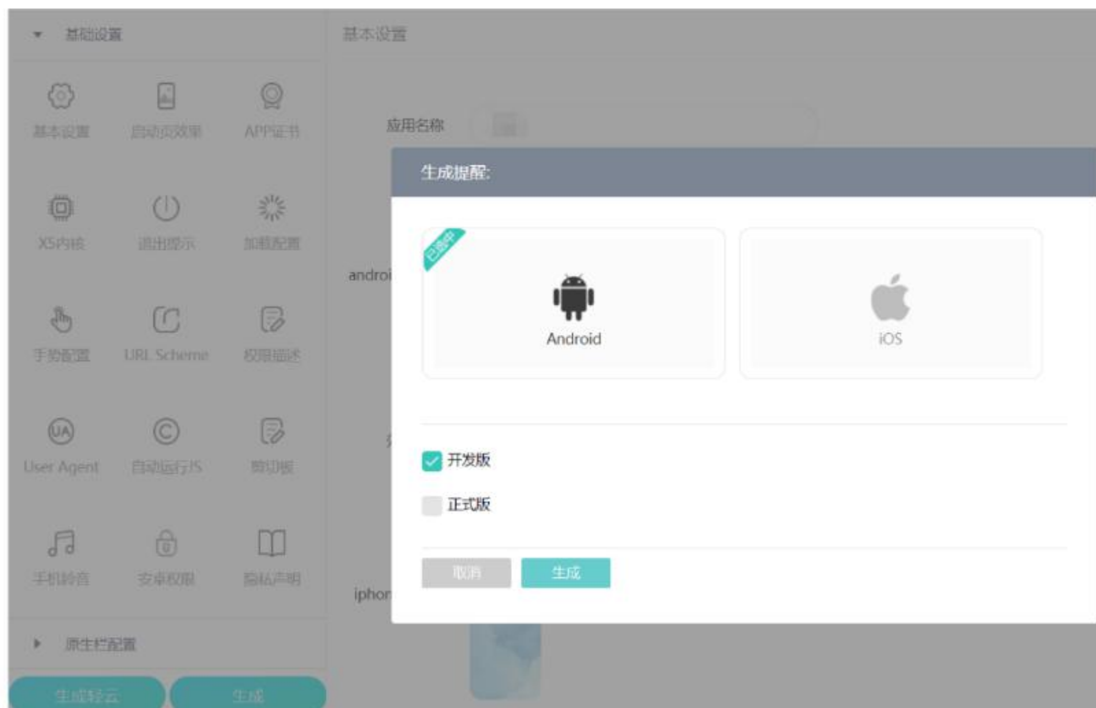
3. 封装平台、分发平台使用流程：

封装类应用由于仅是将网站转成APP，不需要像原生应用进行迭代开发。在封装平台填写应用基本的信息，例如应用名称、应用图标、应用包名，需封装成应用的网站网址，选择应用的基础功能，例如：启动页效果、应用退出提示、权限描述（应用获取手机权限时给予用户的文字提示）即可完成应用的封装。

如下图展示应用封装平台的封装流程：


APP
基础设置
基本设置
启动页效果
APP证书
X5内核
退出提示
加载配置
手势配置
URL Scheme
权限描述
User Agent
自动运行JS
剪切板
手机铃音
安卓权限
隐私声明
原生栏配置
生成轻云
生成
导入
导出
基本设置
应用名称
小白
logo
android启动页
*必填 App启动时展示的图片，点击效果图片可单独替换
效果展示
默认图片
iphone启动页
效果展示


详情
APP
插件
升级
基础设置
基本设置
启动页效果
APP证书
X5内核
退出提示
加载配置
手势配置
URL Scheme
权限描述
User Agent
自动运行JS
剪切板
手机铃音
安卓权限
隐私声明
原生栏配置
生成轻云
生成
导入
导出
APP证书
inid
下载地址
https://www.
安卓包名
com.kuaqkv.kimkzon
使用证书
默认证书
自定义证书
默认证书
自定义证书
默认应用签名 生成后显示
默认签名sha1 生成后显示
默认签名sha2 生成后显示
默认证书别名
默认证书密码
默认证书store密码



部分封装平台在提供基础的封装功能外，还会提供应用权限接口，如通讯录、手机信息、文件上传。网站内编写相关的代码与封装平台的接口对接，封装出的应用就具备相应的权限功能。在用户安装此应用后，通过相关的权限可获取到用户手机的数据信息。



通信录功能模块

调用手机通信录。JSAPI无需引放任何js文件直接调用。

BSL.GetContact('callbackMethod')

读取通信录单个联系人。

参数	必填	说明
callbackMethod	是	自定义回调函数

BSL.GetAllContact('callbackMethod')

读取通信录所有联系人。

参数	必填	说明
callbackMethod	是	自定义回调函数

回调数据

读取联系人数据传入回调函数内。

参数	数据类型	说明
lastName	字符串	姓氏
firstName	字符串	名字
telNums	字符串	电话数组
emails	字符串	电子邮箱数组

应用完成封装后，部分封装分发一体式平台，会提供应用的下载链（二维码）。未提供应用下载链仅提供应用安装包（APK）的平台，使用者需要通过分发平台生成应用的下载链（二维码）进行应用传播。如下图展示，将应用上传到分发平台后，平台提供相应的应用下载链。封装、分发平台的便利，在促进互联网行业发展的同时，一方面也为黑灰产人员提供了便利，成为了虚假应用的加工厂。



（三）利用应用分发平台实施诈骗的方式及其衍生的攻防对策

借助封装、分发平台，黑灰产人员拥有大量虚假应用及应用下载链。一方面如上文提及的，一方面利用云控、子域名搭建虚假网站，生成应用；一方面通过短信混淆，下载链混淆等攻防手段躲避网络安全厂商的识别。再借助各种诈骗话术实施诈骗，套取用户手机内的隐私信息，骗取用户资金。

360手机先赔用户反馈，其在2020年收到了贷款平台客服的电话，以给用户推荐贷款平台放贷为由，引导用户安装“***钱花”应用。用户在该应用申请10万元后，却未收到平台的放款。随后被此客服以贷款会员费、风险客户费、贷款保险费为由，引导向指定银行账户转账，骗取用户资金。通过对此应用分析，我们发现这是一款利用封装平台生成，利用分发平台存储的仿冒贷款平台的应用。

360手机先赔用户反馈，其在2020年在网上交友的过程中认识了网友。对方以请求用户帮其增加直播间关注度为由，引导用户下载“相约”应用，用户安装软件，帮其点完关注后，与对方进行视频裸聊。裸聊完毕后，收到了对方截取的自己裸聊画面及自己手机通讯录信息截图。勒索用户向对方转账，否则将用户裸聊的视频转给用户手机通讯录内的亲朋好友。经过技术分析，该应用是一款使用封装平台制作的应用，且存在上传用户通讯录的行为。

三.博彩诈骗产业链研究

互联网的迅速发展，也吸引了博彩行业的目光。在利益的诱惑下，传统的赌场逐渐将业务分流到线上，低成本、低风险、高回报的博彩行业甚至吸引了众多掌握一定技术能力的人员铤而走险，运用新技术、新手段实施诈骗。相比于常见的网络诈骗，借助博彩平台实施的诈骗具有更“高深”的攻防手段和诈骗话术，被骗资金少则几十元，多则数百万元。

（一）流水线生产模式的博彩平台

通过360诈骗理赔服务收集到的用户举报案例，我们发现电信网络诈骗犯罪一般是针对特定少数人群实施的。在该部分易感人群中，博彩诈骗又是其中最高发的。通过对近半年年的博彩诈骗案件进行分析，发现如下几个共性。博彩平台为什么界面、风格都很相似；博彩诈骗在社会各界重拳打击下，仍屡禁不止；诈骗分子在实施诈骗行为时，受害人何以对诈骗分子的话术深信不疑？

为了解答这些疑问，我们有必要从“包网平台”这一产业链入手，深度挖掘当前信息化时代博彩诈骗的演化趋势、逐步分析博彩诈骗的技术手段、剖析博彩平台的推广策略、解读诈骗分子的话术。

1.环环相扣的包网平台

在移动互联网时代之前，运作一个博彩平台，需要专人开发（博彩网站/应用的前台、运营后台）、接入博彩项目（彩票类、体育类、真人视讯、电子游戏类）、对接第三方支付、搭建防火墙提升风控能力，还需要培养客服、运维、推广、“洗钱”等等。通过此种方式搭建博彩平台，门槛高、难度高、成本高、风险高。

于是提供“建站—维护—活动策划—支付接口—域名—服务器—漏洞防御—反套利—后台系统等一系列与博彩运作”流水线式服务的包网平台粉墨登场。违法分子只需向包网平台支付维护费、开板费、平台盈利分成后就可以使用包国平台的服务。而违法分子需要做的只是像使用CMS（建站系统）一样，先选择网站或APP的页面模板，再修改网站的标题，即可完成博彩平台的搭建。下图为包网平台的搭建流程：



针对不同的博彩游戏，包网平台分别提供不同类型的包网服务，如纯彩（彩票相关的平台）、电竞（电子/体育竞技相关的平台）、棋牌包网、真人包网、综合包网等不同类型。

面对门槛最高的博彩平台运营问题，包网平台还提供集成玩家管理、资金管理、平台管理、图像化展示等功能，帮助运营者掌握网站动态。可以说包网平台将博彩诈骗这一产业链转化为流水线般标准化、模板化、简易化的模式，为公安机关的打击活动带来全新挑战。下图为包网平台提供的博彩平台模板：



2. 恣意妄为的技术支撑

随着通信行业的演进和发展，新的融合型诈骗手段不断涌现，诈骗分子闯入通信行业的价值链，运营商和公安机关正在面临着越来越严峻的挑战。众多的互联网黑灰业务利用备案域名批发商城、境外免备案服务器、网站/应用源码、第三方客服应用、封装封发平台以及第四方支付平台（含资金池）等作为推广、实施犯罪手法的技术手段，并在互联网各个渠道“野蛮”生长。原本是为了方便互联网时代发展，为技术爱好者提供的便捷工具。不曾想竟沦为犯罪分子实施网络犯罪的温床。

在黑灰产攻防的早期，网络安全厂商检测手段较为单一，甚至仅仅通过域名是否含有备案信息，来确认平台真伪。于是黑灰产从业人员会通过一些黑灰产渠道购买已备案域名、免备案服务器、平台搭建源码，从而搭建了可躲避网络安全厂商检测的诈骗平台。

随着网络安全厂商产品能力的提升，传统的黑灰产手法已失效，为解决现状问题。黑灰产逐渐盯上了以第三方在线客服平台、封装分发平台、第四方支付为代表具有移动互联网特征，能够躲避网络安全厂商检测的产品。

（二）环环相扣的推广策略和诈骗话术

1. 掩人耳目的推广策略

在包网平台成熟的流水线上，博彩诈骗团伙已经降低了准入博彩行业的门槛。接下来，对于博彩诈骗团伙而言，最重要的是吸引更多的玩家入场。

于是，短信就成为博彩平台推广的主要媒介。同时v为了应对运营商、企业的识别及拦截，诈骗团伙也在不断变换话术，规避拦截策略。

在短信内容中，以兼职“面试”通过或高佣金为噱头，引导受害人关注指定微信公众号。博彩网站的业务员通过微信公众号的在线客服功能推送博彩网赚项目及博彩平台网址（二维码），引导受害人扫码访问网站。由于短信内容和普通的引导关注微信公众号短信无异，传播时难以被识别为欺诈短信。此类微信公众号传播博彩网站的时候，使用了微信站外网站，导致微信也无法对博彩网站拦截。下图为博彩平台利于微信公众号推广博彩平台的界面：



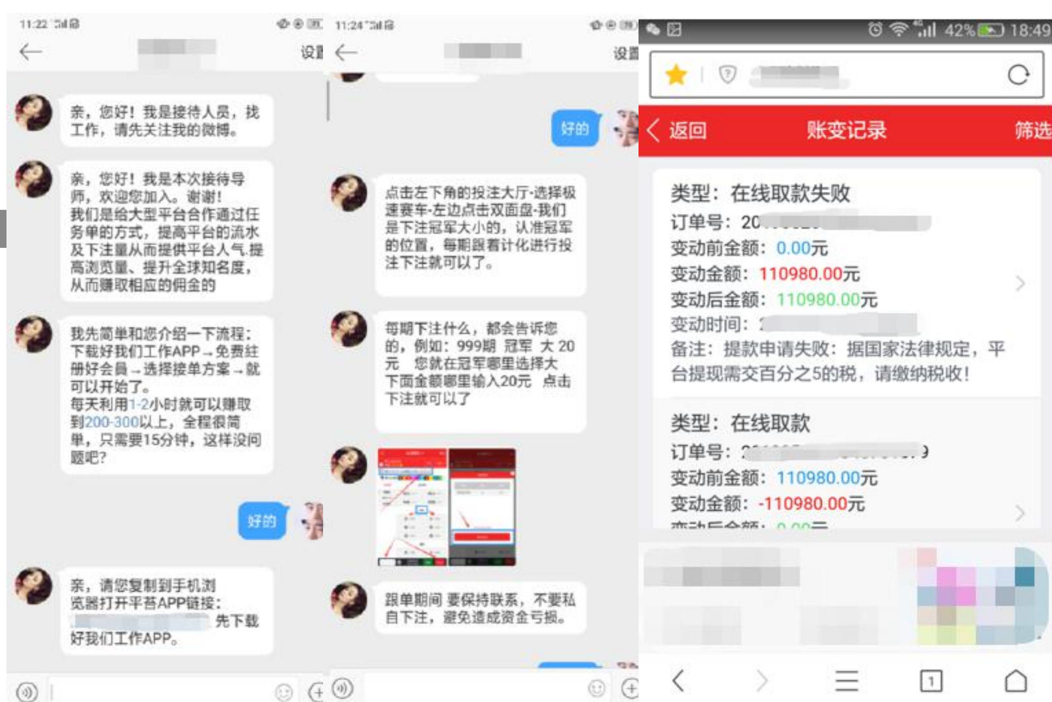


2. 包藏祸心的诈骗话术

相较于传统的网络诈骗，借助博彩平台实施的诈骗过程中，不法分子往往将自身塑造为健康阳光的

形象，或掌握快速、低风险赚钱的方式，或利用虚假的故事，依靠博彩平台的运营人员，取得受害人信任，进而吸引受害人在平台投注，骗取其钱财。

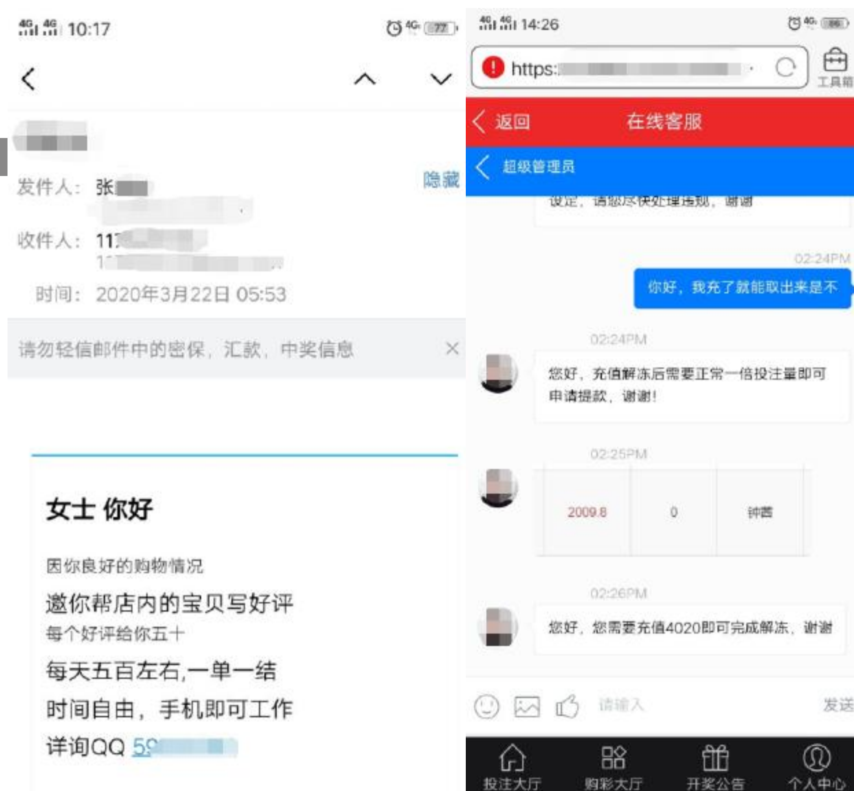
例如以邀请群众参与店铺刷好评，给群众返高额佣金为诱饵，吸引群众的关注。待吸引潜在受害人关注后，犯罪嫌疑人会标识此刷单活动是替博彩平台刷单，通过提高博彩平台的流水、下注量、浏览量从而提高该博彩平台在全球的知名度。随后引导用户安装指定的博彩平台应用。待用户在该平台注册后，给用户发送极速赛车刷单任务（期号+大/小+投资金额），用户在平台充值后，按照对方提供的任务要求购买后，提现成功获得了佣金。随后对方开始给用户发送高额任务，用户按照对方要求，在平台充值巨额资金，盈利后准备提现，但却发现此时已经无法提现。发觉上当受骗。下图为受害人在博彩平台提现失败界面。



第八章 2020年上半年度热门“诈骗剧本”

一.兼职挣钱？实为赌博诈骗！

2020年3月，用户QQ邮箱收到兼职广告邮件，添加该广告邮件中留下的联系方式。与对方沟通后，了解到该兼职项目为彩票跟投，根据指定导师的指引投注可获得盈利。随后用户根据导师指引，在指定时间购买指定项目（例如：大奖五分彩：第204期个位【大】80）。用户前期投注十几元，都盈利了，赚到几十元收益，并成功提现。后期对方将充值门槛提高至100元，用户增加了投注资金，也盈利后，却无法体现，被客服告知用户投注错误，账户被冻结，需要缴纳解冻金，用户按照客服要求充值进行解冻操作，仍无法提现，得知受骗。



专家解读

从诈骗手法上看，网络博彩类诈骗一般会采用前期免费给投注计划，吸引用户投注，后期设置提现金额门槛，或限制用户提现的方式骗取用户充值的资金。从博彩诈骗的手法演变上看，博彩平台逐渐减少对QQ、微信等社交平台的依赖，呈现出利用小众聊天软件作为渠道进行诈骗的趋势，试图降低账号被封风险。

安全警示

天上不会掉馅饼，看似美味的馅饼很可能是陷阱。找到的赚钱“妙计”，仅是骗子放出引导你入场的糖衣炮弹。线上博彩有风险，入场需谨慎。

二.网贷被骗数万元，虚假借贷诈骗又见抬头之势

网贷被骗数万元，虚假借贷诈骗又见抬头之势

为避免疫情进一步扩散，大多人都响应政府的号召，在家度过了一个“漫长”的春节假期。虽然全国各地已完成了复工复产，但疫情还是影响了很多企业和个人的正常收入，企业为现金流担忧，个人为房贷、车贷、信用卡、花呗还款发愁。骗子们也紧盯着疫情的发展，不浪费任何一次危机所带来的“机遇”。

2020年用户收到贷款平台客服电话，在客服的推荐下，安装客服所发送的应用。并在该应用申请10万元贷款（24期，每期还款4766.67元）。随后被此客服以贷款会员费、风险客户费、贷款保险费为由，引导向指定银行账户转账，骗取用户资金。

钱花

申请借款

确认借款信息

借款金额 ¥100000

借款期限 24个月

还款 ¥4766.67（每期）

请签名

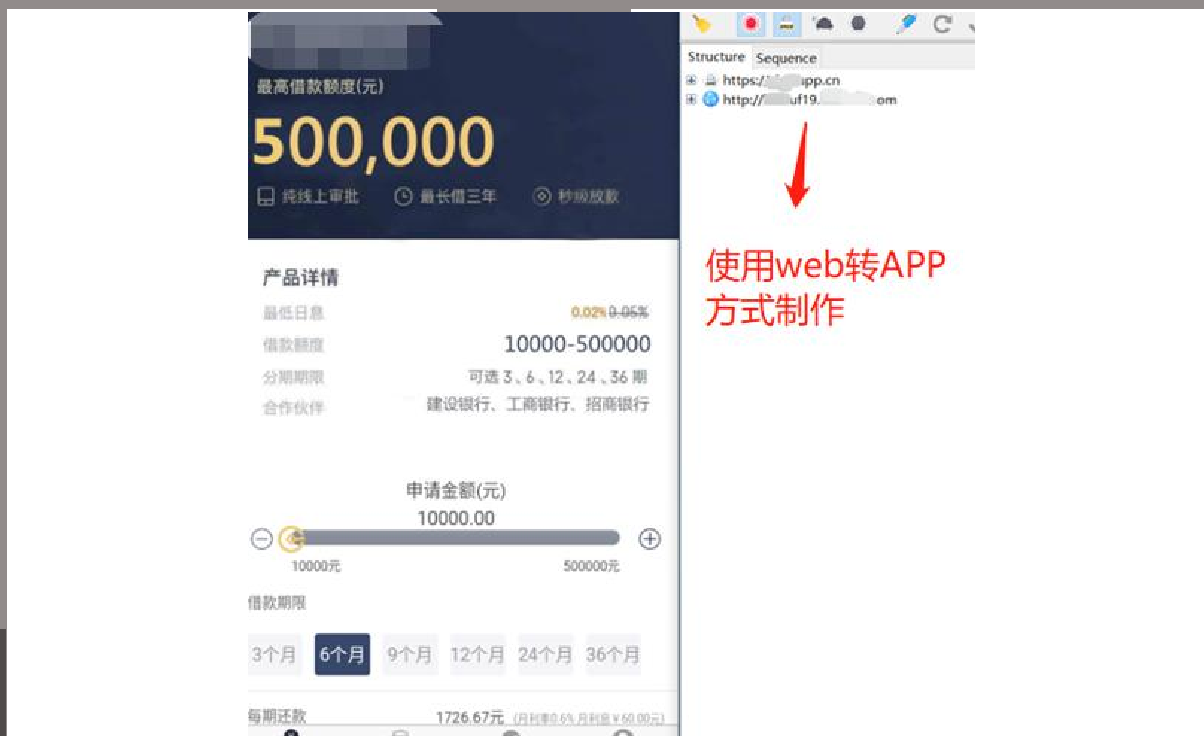
您的申请已受理,可在我的借款中跟进审核进度!

确定

清除 确定

提交借款申请





专家解读

通过对该贷款应用逆向分析，发现该应用是通过封装平台封装生成的仿冒类虚假贷款应用。此类虚假应用虽然能在应用界面模仿“知名”贷款平台，但在具体的功能上，由于其仿冒的本质，仍然会存在明显的区别。

1. 此类应用由于无法上架正规的应用商店，多通过分发平台作为应用的存储平台。

2. 此类应用由于主要作用是实施诈骗工具，非正常的贷款平台，使用此类应用申请贷款时，不会对上传资料进行审核，信息可以随意填写。

安全警示

早些年的借贷诈骗，犯罪嫌疑人往往抓住人们急于用钱的心理，以先收手续费再放款为由骗取钱财。近些年，借贷诈骗开始转变思路，先让用户看到申贷成功，在提现的过程中设置陷阱，引导用户自主转账。凡是在申贷过程中需要缴纳高额费用的贷款平台都可能存在高风险。

大部分金融平台的账户是对公账户，非个人银行账户，因此提供个人账户收款的，绝大多数都是骗子。同时，大部分金融机构，在放贷过程中，也不会以提现银行账号，征信不足、流水不足为由，要求向指定银行账户转账。

三.女网友裸聊背后的“桃色陷阱”

移动互联网的发展，手机应用的普及，加上交友市场的需求旺盛，手机应用市场随处可见各类交友应用。随着“新型冠状病毒肺炎”疫情的出现，人们“被迫”留守屋内，上网交友成了众多的“宅男”消遣时光的选择，出现了众多的裸聊被勒索事件。

不法分子通过社交应用结交用户，以交友为名引导用户添加对方的QQ。在与用户聊天的过程中，使用话术，套取用户的个人信息，如姓名、职业、年龄。以请求用户帮助其增加直播间关注度为由，引导

用户下载指定的虚假“直播”软件。随后以视频裸聊为由，引导用户通过QQ进行视频裸聊，裸聊过程中会特意要求用户露出脸部和下体的画面。视频结束后，给用户发送刚刚的裸聊画面截图（包含用户脸部信息）及用户手机通讯录信息截图，并以会将此视频群发给用户手机通讯录好友为由，勒索用户向对方转账。用户转账后，对方仍未满足，仍反复要求用户转账。



专家解读

不法分子引导用户安装的虚假“直播”应用，存在上传用户手机通讯录的行为。表面看起来是直播应用，但安装后是无法使用直播功能的，只是不法分子用来盗取用户手机通讯录的工具。不法分子借助一些虚拟摄像机软件及色情视频，模拟与用户的裸聊画面，在于用户视频裸聊的过程中，引导用户露出脸部及下体画面，偷录用户的裸聊画面。待获得用户手机通讯录及裸聊画面后，实施敲诈勒索。

安全警示

自古深情留不住、唯有套路得人心。试想那些有美丽头像、动听名字的女子，为何在千万人中主动找上你，假装被你撩？还会主动提出“赤诚相见”？是因为你幽默、贴心、帅气、有钱？都不是，只是因为你好骗。

四.在线破解！冒充网游交易平台实施诈骗全过程

2020年3月用户在某游戏交易平台上架出售自己的游戏账号，之后在该游戏交易平台中收到买家的信息，对方以确认下单需求填写用户信息为由，索要了用户的QQ账号。并给用户发送了“已下单，已用QQ邮箱邮件方式告知卖家发货”的截图。

随后用户QQ邮箱收到了“付款订单”邮件，用户访问了邮件内容中的网站，网站内客服以防止用户不发货为由，要求用户缴纳800元保证金。用户按照客服指引，使用支付宝扫码转账800元。随后客服以用户的积分未达到安全转账为由，要求用户继续转账，用户发现受骗。



专家解读

此类案例中，不法分子先谎称买游戏，通过伪造的图片，索取到了用户的QQ。之后再冒充网游交易平台给用户发送邮件。使用了邮箱的超链接功能（点击文字后跳转指定的网址）。让用户看起来是访问邮件中的www.jiaoyi***.com但点击后实际是访问的是第三方在线客服平台（api.p**800.com/chat/39**?t=0）。骗子使用了第三方客服平台网站伪造了该网游交易平台的客服。

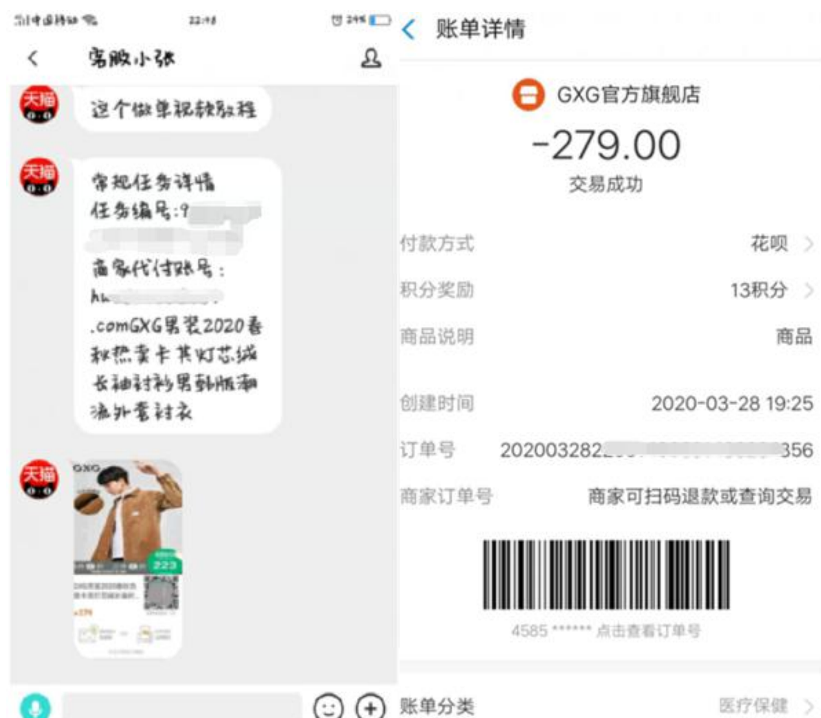
安全警示

网游交易要通过官方交易平台，不要轻信非官方的网游充值优惠，如需购买游戏装备、道具等，要通过游戏官方充值渠道进行游戏充值，非官方的网游充值优惠渠道大多是骗子。切勿轻信“先支付”，支付、转账等是向对方直接付款，一旦遇到虚假交易，很容易造成经济损失。

五.刷单再现支付陷阱，“高倍镜”找出破绽！

用户在QQ群，看到兼职刷单广告，联系对方后，对方给用户描述刷单流程：“使用淘宝搜索指定的商品，将商品加到购物车后，使用支付宝扫码指定商家的收款二维码，扫码后，会出现输入验证码及企

业代付的字样，选择企业支付后，即可完成刷单操作”。但用户实际操作时，扫描指定商家收款二维码、输入支付宝支付密码后即支付成功，并未出现验证码及企业代付界面。用户多次操作后，仍未获得本佣金，发觉受骗，联系对方后，对方给用户发送“退款”客服的支付宝联系方式，用户添加该退款客服后，对方未退款，仍引导用户继续刷单，用户得知受骗。



专家解读

从诈骗手法上看，此诈骗手法与以往刷单诈骗手法相同，均是通过冒充电商平台商家，引导用户扫描指定二维码进行支付，但在细节上做的更加逼真，比如通过多种方式打造同名商家名称。

通过研判分析可以发现，真实的店铺为服饰类商家，收款为企业，而骗子仿冒制作的店铺其分类为医疗保健商家，收款方个人，两者仅仅是名称相同。t

安全警示

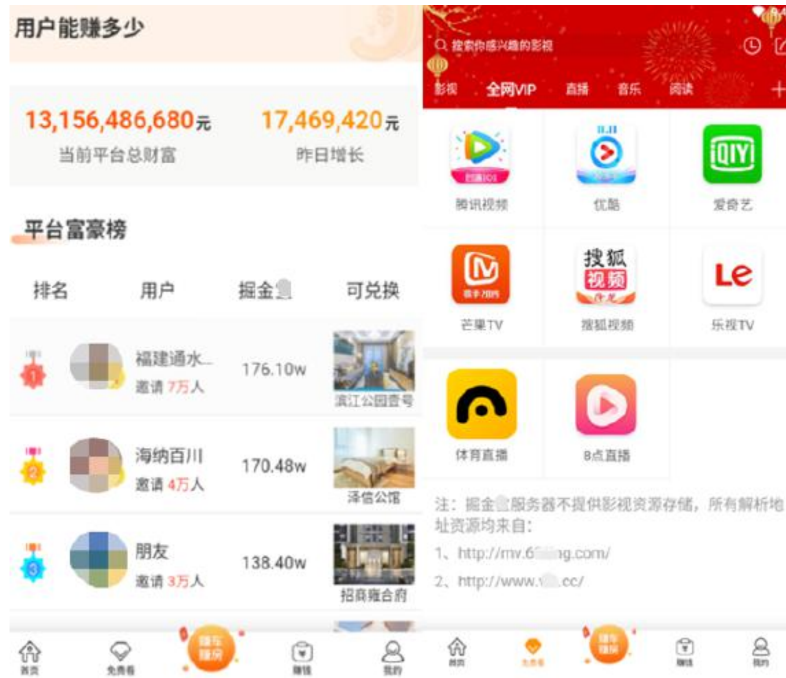
网赚基本99%都是骗局，任何让交纳保证金的兼职全部不要相信！对于轻易可以“获取高额回报”的工作要保持高度警惕，不要抱有侥幸心理。如果被骗，及时收集相关证据，如：聊天记录、交易记录等，并立即报警。

六. “万亿”市值还给原始股，虚拟货币平台背后的“套路”

近几年，互联网虚拟货币产品营销有个特点。先造势画大饼、再雇“水军”给用户“洗脑”，造成产品易赚钱，用户能够“一夜暴富”的假象。一款号称6个月内上市交易，市值可达万亿的虚拟货币平台“掘金*”吸引了众多的“粉丝”。该应用主打热门资讯（号称精选全网优质媒体号，杜绝垃圾新闻）、免费影视（号称拥有全球最大最全影视片库，不需要会员就能看各大影视平台VIP专属视频）、赚房赚车（在应用内每天阅读、分享文章、邀请新用户，即可获得平台货币掘金*，该货币等价于公司原始

股。待平台上市，可套现获得巨额资金）。可以看出，这是一款集免费VIP视频、看新闻赚钱、“拉人头”获收益、平台货币玩法的聚合类平台。

下图为该应用展示的用户收益排名截图，第一名邀请好友注册数量7万，获得176.1万掘金*货币，货币可兑换滨江公园壹号房产，及应用主打的免费影视功能截图：

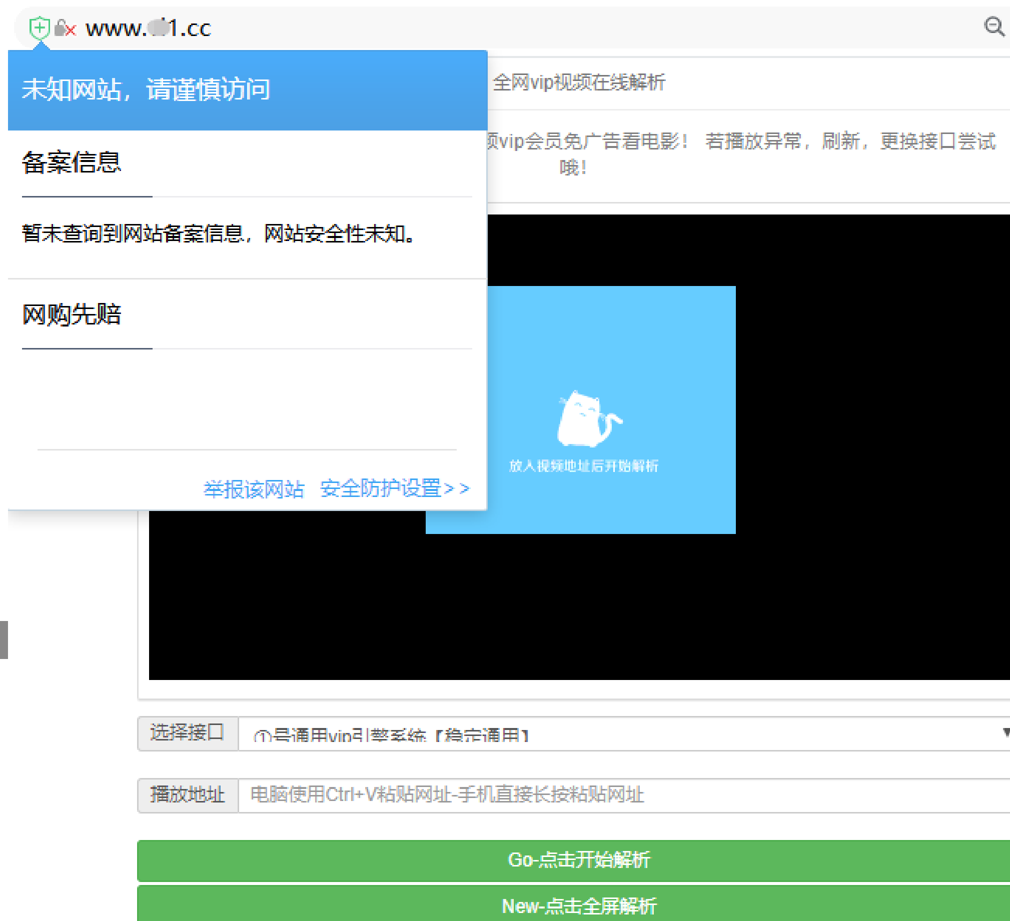


专家解读

平台运营至今的周期，早已超过平台宣传的6个月内上市交易，但上市计划遥遥无期。实际上该应用背后的注册公司其注册资本仅10万元，根本达不到企业上市的要求。

注册资本	10万人民币	实缴资本	-	评分 47
成立日期	2018-07-09	经营状态	存续	
统一社会信用代码	9144[illegible]M	工商注册号	4403[illegible]5	
纳税人识别号	9144[illegible]M	组织机构代码	MA[illegible]	
公司类型	有限责任公司	行业	软件和信息技术服务业	
核准日期	2018-07-09	登记机关	福田局	
营业期限	2018-07-09至无固定期限	纳税人资质	-	
人员规模	小于50人	参保人数	4	
曾用名	-	英文名称	-	
注册地址	深圳市[illegible]2 附近公司			
经营范围	计算机信息科技领域的技术研发；经营电子商务；数据库服务、数据库管理。（法律、行政法规、国务院决定禁止的项目			

平台宣传的免费VIP影视功能，如下图展示，实际上是使用了域名都未备案的盗播电影网站的资源。盗版电影网站本身是违法违规的，号称将要上市的公司，使用的却是违法违规的产品，这本身就是存在矛盾的。



平台宣传的“赚房赚车”，主打的功能就是拉下线邀请好友注册该应用，获得平台的虚拟货币（等价于公司原始股），待公司上市，用户即可完成套现操作。但实际上虚拟货币本身没有任何价值，价值体现的前提条件是市场承认其价值，但通过前面的分析，我们知道这样一个既达不到上市要求，又存在违规产品的平台本身都是存在问题的，更谈不上说市场承认其平台货币价值。

安全警示

目前市面上不少平台打着虚拟币、数字货币的口号，本质就是为了引导用户不断拉下线获利，表面干着炒高虚拟货币价值，私底下却干着大量卖币套现的勾当！擦亮双眼，多方鉴别，切勿轻信！

第九章 2020年上半年度网络安全行业动态

一.工信部：做好疫情防控期间信息通信行业网络安全保障工作

今年2月份，工信部办公厅发布关于做好疫情防控期间信息通信行业网络安全保障工作的通知，称要加强重点用户网络安全技术支撑，加强重点地区网络基础设施安全防护。

工信部表示，加强涉疫情重点保障地区网络基础设施、重要域名系统等安全防护，利用远程检测等技术手段，强化对重点区域的网络安全风险评估和隐患排查，为疫情防控指挥调度、医疗救助、远程办公和人民群众生产生活提供安全可靠的基础网络服务。

要加强涉疫情网络安全威胁监测处置，按照公共互联网网络安全威胁与处置工作机制，对伪装成疫情信息传播网络病毒或相关钓鱼网站、恶意邮件、恶意程序，以及医疗机构、疫情防控物资生产企业所属网络系统存在受控、漏洞等情况加大监测力度，利用网络安全威胁信息共享平台及时通报有关情况，发布风险提示，协助相关单位采取有效处置措施，从源头上降低网络安全风险，维护疫情防控期间的网络秩序和公共利益。

同时，要加强疫情期间电话用户入网服务保障。鼓励基础电信企业、移动通信转售企业通过网络渠道为用户办理电话入网实名登记手续，引导广大用户利用电信企业门户网站、手机APP、掌上营业厅等线上方式办理电话入网手续及手机卡。基础电信企业、移动通信转售企业应加大对网络渠道销售手机卡业务及办理流程的宣传，做好相关业务系统和平台的保障，切实为广大用户提供便利。

工信部还称，要充分发挥电信网、互联网诈骗技术防范系统等技术平台作用，切实强化对涉疫情诈骗电话、短信的精准分析和依法快速处置；针对涉防疫医疗物资购买、航班行程退改签等诈骗新手法新套路，及时研判预警，对相关涉诈网站、域名、APP、账户依法快速处置。进一步加强与公安机关工作配合和信息沟通，及时通报涉疫情电信网络诈骗信息线索。充分利用微信、微博、短彩信、APP等平台开展涉疫情电信网络诈骗的宣传引导和风险提示。①

二.公安部部署开展“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役

5月7日上午，公安部部署全国公安机关开展“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役。北京、河北、上海、江苏等15个省市公安机关，同步开展了集中收网行动。“云剑-2020”集中收网行动截至7日15时，各地共捣毁为贷款类电信网络诈骗犯罪团伙提供服务的违法1069短信平台57个，抓获犯罪嫌疑人798名，扣押手机、银行卡、电脑等一大批作案工具。



今年以来，公安机关在工作中发现，通过伪造虚假贷款App，以缴纳手续费、保证金为由，对有贷款意向群体实施贷款类电信网络诈骗案件多发高发，危害严重。公安部成立工作专班，对此类违法犯罪活动开展集群战役，实施专项侦查打击。

经初查，一些有资质的1069短信平台披着合法的“外衣”，干着非法的“勾当”，违规将1069号码层层转售、层层代理，为贷款类诈骗犯罪团伙等提供各类服务，并已成为犯罪链条中不可或缺的关键环节。

据了解，2019年6月到今年1月底，公安部部署开展的“云剑”行动，全力打击电信网络诈骗、民族资产解冻类诈骗和套路贷等突出犯罪，强力追捕逃犯。2019年共侦破电信网络诈骗案件20万起，抓获嫌疑人16.3万名；打掉民族资产解冻类诈骗犯罪犯罪团伙620余个，抓获犯罪嫌疑人1.1万名；侦办套路贷案件5320起，抓获嫌疑人5.1万名；追逃工作取得历史最好成绩，抓获在逃人员46.9万名，其中公安部A级通缉令逃犯139名。公安部有关负责人表示，公安机关将继续保持对贷款类电信网络诈骗违法犯罪的严打高压态势，并会同有关部门进一步加强监管治理，坚决维护人民群众财产安全和合法权益。②

三.公安部打击治理跨境赌博取得阶段性显著战果

1.自2月28日部署打击治理跨境赌博工作专题会议以来，公安部部署全国公安机关迅速行动，深入开展打击治理跨境赌博工作，严厉打击跨境赌博及与其关联的涉黑、诈骗、洗钱、绑架、拐卖、偷渡、金融等违法犯罪活动，取得明显阶段性成效。截至目前，公安部挂牌督办案件79起，各地公安机关侦破跨境赌博案件257起，抓获犯罪嫌疑人11500余名，已移送起诉1530余人；摧毁涉赌平台368个、技术团队148个，打掉支付平台和地下钱庄187个，查扣涉案银行卡22万余张、冻结涉案账户28100余个，查明涉案资金2290余亿。另有一大批参赌人员依法受到处理，一大批涉赌人员被列入出入境黑名单。同时，针对涉跨境赌博和电信网络诈骗犯罪银行账户黑灰产业，各地公安机关持续开展集中打击整治行动，捣毁窝点1200余个，缴获涉案账户2.7万余套，会同相关主管部门查处问责银行和市场监管部门工作人员200余人。



2.在这次公布的典型案例中，有的是境外赌场在我境内揽客招赌，如甘肃公安机关侦破的“1·19”跨境赌博案，犯罪嫌疑人组织代理人员在境外窝点和境内通过网络招揽境内人员参赌；有的是为跨境赌博犯罪提供技术支持，如广东珠海侦破的“4·21”网络赌博案，犯罪嫌疑人以软件研发为幌子，为东南亚等境外赌场及网络赌博团伙提供技术支持；有的是为跨境赌博犯罪提供资金结算服务，如黑龙江牡丹江侦破“933”案件，犯罪嫌疑人在境内对线上赌资进行转移提现，并雇人将现金送至境外赌场；有的是组织出境赌博，如云南临沧公安机关侦破的杨某某等组织人员偷渡出境赌博案等。

3.公安部有关负责人表示，跨境赌博严重危害人民群众合法权益，严重危害经济安全、社会稳定和国家形象。公安机关将始终坚持“零容忍”，坚决依法从严从重打击跨境赌博犯罪及关联犯罪，斩断跨境赌博“资金链”、“技术链”、“推广链”、“人员链”，并与有关部门密切协作，深入推进各项治理工作，同时加强与相关国家执法合作，坚决扭转跨境赌博犯罪高发态势。公安机关正告组织和参与跨境赌博违法犯罪活动的人员，立即停止违法犯罪活动，主动投案自首。希望广大人民群众认清跨境赌博“十赌十骗”、“十赌十输”的骗人本质和严重危害，自觉抵制赴境外或在网上参赌，不断提高防范意识和能力。公安机关欢迎广大人民群众积极检举揭发相关违法犯罪行为，并将依法保护举报人的个人信息及安全。③

四.犯罪团伙利用“裸聊”敲诈勒索

今年4月份，福建警方陆续接到警情，报案人称在网上直播间进行网络裸聊后被人敲诈勒索钱财。警方通过进一步侦查发现，受害人将钱款打入嫌疑人指定的账户后，这些钱又通过了多个账户的流转，最终在南宁的自动柜员机上被人取走。警方经过摸排调查，掌握了一个以嫌疑人王某为首的犯罪团伙的基本情况。

警方了解到，嫌疑人会在一些网络群里发布色情网站的信息，并在这些信息里植入木马病毒，对方在观看不雅信息时，如果做出了一些出格的举动，木马软件就会拍下整个过程，随后嫌疑人则表示要把不雅视频发给当事人的亲朋好友，以此来要挟索要钱财。受害人本以为能破财消灾，不料转款后仍然会被纠缠。



据嫌疑人王某交代，他接受一个自称是台湾人“李老板”的聘用，并按照“李老板”的指示来到了南宁，他们在南宁的这6人仅仅负责取钱，如果有取钱任务的话，王某就安排人出去。今年4月份以来，王某等6人取回的钱款，初步统计大概有1000多万元。目前，6名嫌疑人已经移交福建警方处理，案件还在进一步调查中。④

五.工信部：纵深推进App侵害用户权益专项整治

互联网信息时代，大数据应用带来了机遇与便利，也带来了用户对自身隐私安全的担忧。2019年，APP专项治理工作组开展了APP违法违规收集使用个人信息安全评估，发现一些APP存在强制授权、过度索权、超范围收集个人信息等问题。特别是，一些知名APP侵权“店大欺客”，比如，2020年5月工信部网站发布《关于侵害用户权益行为的APP通报（2020年第一批）》显示，累计16款APP尚未完成整改。如此语境下，一些手机App频繁强制跳转启动、自启动、关联启动，甚至高频次访问手机照片和文件，读取手机信息，表明APP侵权愈演愈烈。⑤

7月29日，工信部召开会议部署开展纵深推进App侵害用户权益专项整治行动，切实加强用户个人信息保护。

此次行动重点对“手机应用软件App、软件工具开发包SDK违规处理用户个人信息”“设置障碍、频繁骚扰用户”“欺骗误导用户”“应用分发平台责任落实不到位”四方面10类问题进行集中排查。按照行动计划，2020年8月底前全国APP技术检测平台管理系统将上线运行，提升自动化检测水平和能力，12月10日前完成覆盖40万款主流App检测工作。同时，整治惩处力度也进一步加大。中国信通院标准所产业互联网研究部主任汤立波：发现问题之后，我们在要求在5个工作日之内完成问题整改。如果没有按照规定完成整改或者是整改不彻底，会通过社会公告、然后组织下架以及行政处罚的方式来进行进一步处罚，纳入到电信业务经营不良名单或者是失信名单。⑥

六.工信部发布工作方案运用大数据技术防治电信网络诈骗

工业和信息化部19日在官网公布了《关于运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》，提出将充分运用大数据等新一代信息技术强化电信网络诈骗精准治理、有效治理，加快健全完

善行业防范治理长效机制。[6]

当前，电信网络诈骗方式和手法不断翻新，诈骗活动呈现从电话诈骗向互联网诈骗、从全国分布向重点边境地区集聚、从“短平快”诈骗向长线套路诈骗转变等趋势特点，技术对抗性日益加大，亟需运用大数据推进构建长效机制，为行业防范治理工作提供更加有力的数据支撑和能力支撑。

方案围绕技术平台、监管能力、工作机制，明确了相关具体工作任务。

比如，在提升监管能力方面，方案要求强化事前预防能力建设，建立全网疑似涉诈网络资源交叉核验机制，对高危码号、IP地址、域名等及时清理整顿，提早防范化解涉诈风险；强化事中责任督导机制建设，深化企业责任清单管理，完善问题通报和公开曝光机制，探索实施行业涉诈失信企业“黑名单”，有效落实企业主体责任；完善事后反诈成效评价体系，完善基础电信企业防范治理电信网络诈骗评价指数，研究重点互联网企业防范治理电信网络诈骗评价指标，客观准确评价治理成效。[7]

第十章 社会责任

一. “安全大脑”助力抗疫反诈工作，配合工信部守护用户移动安全

1. 疫情期间的手机安全“狙击战”

突如其来的新冠肺炎让2020年一季度成为很多人终身难忘的记忆。在万众一心抗击疫情的过程中，360坚守在网络世界，守护大众的信息安全，担当着互联网安全卫士的忠实职责。在2020年第一季度我们利用信息安全的角度，分析了疫情期间的移动安全状况，为民众的工作生活敲响了警钟。

为积极响应工信部印发《关于做好疫情防控期间信息通信行业网络安全保障工作的通知》的　工作要求，360手机卫士在疫情期间针对各类不法信息传播动向进行实时监控，协助工信部等机关单位做好疫情防控期间违法诈骗等不法信息的拦截治理工作。针对违法诈骗等不法信息的“新变种”适时调整线上拦截策略，遏制其传播态势，实现精准打击。

在2月4日，360手机卫士疫情工具箱上线，涵盖“交通出行”、“医疗健康”、“社会关怀”、“官方联系”四大板块，倾尽全力为全国用户提供各类防疫支持与服务。在“工具箱-口罩查询购买”板块中，用户只需选择所在地，即可查看360整合全网资讯提供的，该地区口罩等防护用品现货及补货的预约、购买与取货等信息。与此同时，用户可点击下方浮窗，查询了解所有已取得医疗器械相应资质的，可在国家食药监局网核验的防护用品企业信息。若大众用户需要第一时间与各类医疗等防疫机构获得联系，寻求帮助，可在“官方联系-疫控电话查询”工具中，查询拨打全国疾病预防控制中心的突发公共卫生事件应急热线，与全国卫健委官网、全国24h免费心理援助和投诉举报热线等国家相关官方防疫渠道取得联络。



省	疾控中心	咨询电话
北京市	北京市疾病预防控制中心	010-64212461
天津市	天津市疾病预防控制中心	022-24333453
河北省	石家庄市疾病预防控制中心	0311-86032070
	唐山市疾病预防控制中心	0315-3252542
	秦皇岛市疾病预防控制中心	0335-3652607
	邯郸市疾病预防控制中心	0310-8168129
	邢台市疾病预防控制中心	0319-2130065
	保定市疾病预防控制中心	0312-3353111
	张家口市疾病预防控制中心	0313-4099500

毫无疑问，2020年的一季度，一定会被我们永远铭记。而在虚拟网络，从手机信息安全的数据维度，也真实记录了这个阶段的丑与恶、善与美。如今，我们越来越离不开信息网络，而网络信息安全也必将成为我们重点关注的领域。从疫情期间的网络安全态势中可以让我们得到很多警醒、很多启发，也让我们看到了360作为网络信息安全企业的担当和价值。

2. 反诈数据推送，时刻关注不法信息传播动向

针对当前电信网络诈骗日趋精准化、体系化的现实，跨行业协同治理成为趋势，360积极配合中国信息通信研究院开展反诈骗工作。通过对钓鱼网址、电话、短信和恶意应用的风险分析，将涉诈数据识别后推送到信通院，监管部门可以通过涉诈数据，一方面掌握实时的诈骗信息进行预警，还能根据诈骗数据进行态势分析，并结合警方、运营商、互联网公司等渠道数据，结合人工智能、机器学习等手段，开展针对诈骗数据建模分析治理工作。

当前电信及网络诈骗犯罪多发，例如比较常见的冒充淘宝客服、杀猪盘、贷款诈骗等都涉及诈骗分子利用话术诱导受害人到各网贷公司贷款，导致受害者自有资金被骗后，受害者还通过各网贷平台进行贷款，造成受害人和各网贷公司重大财产损失，严重者甚至造成个人极端事件。360手机卫士通过大数据分析以及对黑产链条研究，掌握了重点诈骗类型在传播、制作阶段的特点，在传播端，通过对短信文本攻防的特点进行专项识别云规则的部署，同时对境外号码、短信平台为发送号码的诈骗短信进行重点分析，及时优化防护策略，保证精准有效的识别诈骗短信，并将数据与信通院、运营商共享，协助在传输端进行阻断的工作。

3. 工信部防诈宣传，警惕网贷诈骗

为配合工信部网安局发起的《防范电信网络诈骗宣传稿件征集计划》工作，360作为轮班单位，第一篇投稿《【提醒】网贷诈骗难防范？且慢，先来看看这份防骗指南！》已成功过审并发布上线，获得网安领导的高度肯定。疫情期间网贷诈骗呈现高发态势，通过解读网贷诈骗的施诈流程，总结手法实施中的要点、疑点，呼吁大众警惕网贷诈骗，以防受骗。同时在疫情持续期间，为配合工信部网安局发起的《防范电信网络诈骗宣传稿件征集计划》工作，360作为轮班单位，第一篇投稿已成功过审并发布上线，获得网安领导的高度肯定。文章通过图文的方式，通俗易懂的呈现给大众如何来识别贷款诈骗，针对贷款诈骗高发的现象，解读了此类诈骗套路，提醒大家要做好诈骗的预防工作。

在疫情的持续过程中，黑灰产业中蠢蠢欲动，涉及疫情的各类诈骗频频发生。为积极做好疫情期间防骗宣传工作，360手机卫士针对“疫情防骗”系列发布并传播诈骗案例20余篇，均篇阅读覆盖约10W+的手机用户，以防遭遇不法分子的诈骗侵害。同时发布《3·15防诈骗科普全攻略》、《2019年中国手机安全状态报告》在社会各个传播渠道进行曝光，协助读者了解当下移动安全趋势，普及安全防骗知识。

二.协助公安机关，打击黑灰产业链初见成效

1. 虚假贷款平台遭公安机关严厉打击

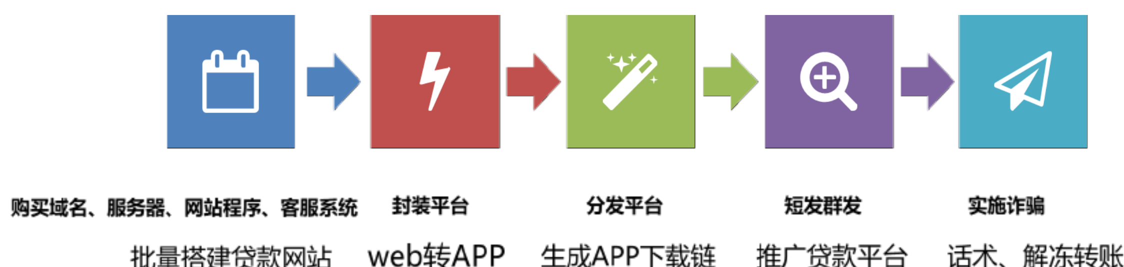
伴随着互联网行业从PC互联网时代发展到移动互联网时代，黑灰产业也从PC互联网时代的“单兵”作战向移动互联网时代的“集团化”作战转变，其网络安全技术及攻防策略不断演进升级。

现如今，网络借贷诈骗手法逐渐多样化，新途经层出不穷。其中曾被315晚会曝光过的“714高炮”，具有放贷周期短、放贷金额低、申贷利息高的特点。借贷后，放贷平台会诱导用户续贷，再给申贷者推荐其他现金贷平台，通过拆东墙补西墙的方式还款，最终申贷者将完全落入平台的“圈套”，永远无法将贷款完全偿还。此时平台还会将借贷合同打包贩卖给职业贷款催收公司，并使用群呼电话、短信等手段轮番轰炸。⑧

此外还有冒充知名借贷平台的虚假平台出现，在引导用户安装指定借贷APP后的提现过程中，平台会借由用户账户被冻结、用户征信不足等一系列话术要求持续转账，但始终不放款；或是使用虚假借贷合同，冒充知名借贷公司，以用户征信和银行流水不足为由，要求用户向指定银行账户转账刷流水；再者以注销贷款为名，引导用户在多个借贷平台申贷，骗取所贷资金；还有不法分子冒充借贷催收平台，骗取借贷还款。

5月7日上午10时，随着公安部一声令下，全国公安机关“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役正式打响，北京、河北、上海、江苏等15个省市公安机关同步开展集中收网行动。截至7日15时，各地共捣毁为贷款类电信网络诈骗犯罪团伙提供服务的违法1069短信平台57个，抓获犯罪嫌疑人798名，扣押手机、银行卡、电脑等一大批涉案工具。⑨

360手机卫士作为移动安全领域领先的安全类软件，在配合公安机关进行贷款类专项打击工作上也积极发挥着自身的技术优势。随着技术的升级，贷款类诈骗策略演变为滥用提供后端服务的平台，实现对虚假借贷APP的批量化生成，后由云控的方式转向通过不同子域名的方式生成不同的网址，实现单一网站被拦截后快速上线新网站的目的，同时不法分子开始利用“虚假”认证信息，将第三方客服系统接入到黑灰产平台，为虚假平台提供在线客服服务。



针对贷款诈骗利用黑色产业链条进行制作、伪装、分发来实施诈骗的特点，360手机卫士依靠“应龙反诈综合平台”的大数据分析和关联能力，实现了在诈骗短信传播端识别、钓鱼网址识别和拓线、贷款诈骗应用沙箱分析的黑产链条全打击的能力。在公安机关“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役的配合工作中，360“应龙反诈综合平台”通过对贷款类诈骗网址的拓线和识别，依靠APP沙箱分析能力对贷款诈骗应用的逆向分析，协助公安机关在恶意网址阻断，贷款应用分发平台、封装平台的治理，实现了对贷款类诈骗在黑产链条的全方位打击。

2. 电信诈骗案件溯源支撑

自2020年1月至7月，360“应龙反诈综合平台”协助各地公安机关分析研判电信诈骗案件240余起，针对高发的贷款诈骗、杀猪盘、色情裸聊诈骗等案件进行深度溯源分析，依靠应龙平台数据关联能力，对涉诈类网址、应用和短信进行关联和溯源分析，挖掘出涉诈产业链中相关信息，从而协助公安进行案件的研判和落地。

“您的ETC认证已失效，请点击该网址进行激活”近段时间不少办了ETC的车主收到类似这样一条短信，很显然，这又是一种新类型的电信诈骗——冒充ETC认证短信诈骗。今年5月以来，此类诈骗犯罪不断在全国各地出现，仅长沙范围内就发生此类案件90余起，为有效遏制此类案件的高发态势，长沙市公安局依托专业警种优势，开展专案攻坚，于近期成功破获了一起冒充ETC认证短信诈骗案件，在全国尚属首例！⑩



在此期间，360手机卫士团队通过应龙反诈平台的大数据拓线和溯源能力，对涉诈域名的WHOIS信息、备案信息进行查询，域名关联子域名、同源域名进行查询，同时获取URL指向站点的标题，网站类型等协助长沙公安局专案组进行深度研判分析，专案组通过克服重重困难，逐步发现一条完整的涉及海南儋州、琼海，河南商丘、浙江温州等地的ETC诈骗犯罪产业链，并摸清了该犯罪链条的人员身份、组织结构及活动轨迹。



7月15日下午，在当地警方的配合下，专案组40余名警力在海南儋州、琼海、河南商丘三地同时开展收网行动，共计抓获嫌疑人19名，并查获作案手机30余部，电脑3台，公民信息5万余条。



三.关注女性人身安全，发起女性安全公益行动

当前,针对女性的违法犯罪案件时有发生，特别是侵犯女性隐私的违法事件尤为突出。对此，除了全社会共同努力营造更加安全的公共环境外，借助科技力量更好地守护女性个人隐私空间同样重要，作为国内最大网络安全企业的360，有着不可推卸的企业使命和社会责任。

专注移动安全领域的360手机卫士，持续致力于实现用户安全的有效防护。针对社会现状，我们在维护用户移动安全的同时，已开展对用户人身安全的防护。此前上线的女性守护中心，便是360手机卫士通过科技手段，倡导女性使用网络安全技术产品，防范和抵御针对女性的违法犯罪，希望借此唤起女性的自我安全防范意识，增强女性自我保护的基本能力。



360手机卫士的“女性守护中心”,基于“虚拟报警器”、“手机防移动保护”、“伪装来电”、“摄像头检测”四大功能,可有效实现安全事件预警、隐私保护、安全脱身、防偷窥偷拍等安全场景,全方位守护女性个人安全。

以摄像头检测功能为例，用户只需在360手机卫士女性守护中心中“一键检测”，就能发现隐匿在暗处的针孔摄像头。该功能依托360安全大脑的赋能，通过对联网摄像头的连接特征、通信方式等进行分析，从而判断当前WIFI下是否连接可疑的摄像设备，能够帮助用户，特别是女性朋友在最短的时间内分辨出当前环境是否存在类似的安全隐患。



存储在手机相册里的证件照、照片里的位置记录、短信里的消费记录信息，很可能让你变成“透明人”。日前，360手机卫士推出“隐私防泄露”功能，针对用户手机相册、位置信息、消费记录短信等个人隐私泄露高危点和盲区，打造“三重防护”，帮助用户避免隐私“裸奔”。

“当前智能手机普遍存在三大隐私泄露风险点，一是保存了含有个人敏感身份信息图片的手机相册；二是手机照片里可能保存的用户位置记录；三是包含消费记录、支付验证等信息的短信。”360安全专家表示，这些隐私信息也是用户容易忽略的盲点，且直接关乎用户的财产安全和人身安全。



据悉，针对以上三大隐私泄露高危盲区，360手机卫士此次“更新”主打三大安全能力。第一项能力“对症”手机相册中的隐私照片泄露风险，这些照片主要包括存储在用户相册中的身份证、驾驶证等包含隐私信息的证件类图片，一旦被盗用后果严重。360手机卫士可及时提醒用户进行处理，降低泄露风险。

第二项能力则聚焦于防范用户位置记录泄露。当前几乎所有智能手机的拍照功能，都具备识别拍摄位置的能力，而一旦这些包含用户位置的照片被泄露或者发布到社交网站上，就暴露了拍照者的地理位置及相关信息。因此，360手机卫士为用户提供了“检测”和“擦除”两种功能，用户可以通过扫描检测出包含位置信息的照片，并及时擦除照片原数据中的完整位置信息，避免泄露。

第三项能力则聚焦于降低用户的消费记录泄露风险。虽然当前社交软件不断普及，已经逐渐替代了手机的短信功能，但是短信依然承担着很重要的用途——银行、支付软件的短信验证功能。360手机卫士的隐私防泄露功能利用对历史短信的深度扫描，检索出其中可能存在泄露个人身份及财产信息的短信，并及时提示用户进行处理，为用户建立起“协查、警报、处理”的全方位守卫措施。

在做好用户隐私防护的同时，360手机卫士也一如既往严守隐私防护底线。“用户在使用隐私防泄露功能前，我们会充分保障用户知情权，只有获得用户授权，我们才会对用户相册、短信等信息进行扫描，而且扫描行为只在本地进行，不会对数据进行任何传输”，360手机卫士相关负责人强调。

隐私泄露是当前亟待解决的问题。不久前，某远程视频会议软件发生用户信息泄露事件，引发大众担忧。此次360手机卫士推出的“隐私防泄露”功能正当其时。

实际上，近期360在守护用户隐私方面频出“重拳”。2019年10月，面对高发的偷拍事件，360手机卫士宣布推出“摄像头检测”功能，帮助用户发现隐匿在暗处的可疑摄像设备。这一功能主要通过对联网摄像头的连接特征、通信方式特征做分析，从而进行识别。该功能填补了移动安全领域在个人隐私方面保护的空白。

“隐私安全已经成为移动安全领域的重要一环，隐私一旦泄露就可能酿成严重的安全事件”，上述360手机卫士相关负责人表示，360将针对用户隐私泄露的痛点、盲点，充分利用360安全大脑的尖端技术优势，发挥360手机卫士在移动安全领域的十余年积累，为用户打造更完善更贴心的移动安全服务生态。

第十一章 提高电信网络诈骗防范与治理策略

一.不断完善技术策略，加强产业链治理打击

黑灰产在技术、话术等多方面，不断完善其自身的诈骗手法，防止在实施诈骗的过程中被识别。如诈骗团伙在使用未含备案信息的域名被安全厂商识别出诈骗特征后，转而开始利用含有备案信息的域名来躲避安全厂商对于欺诈类域名的识别，双方呈现出动态博弈的特征。

面对此种现象，安全厂商不能仅仅“盯着”实施诈骗的样本本身进行事后拦截，还需要从黑灰产业链的角度看待诈骗事件。如针对诈骗团伙使用的备案域名，需了解备案域名的来源、原理、买卖方式。一方面拦截售卖渠道、一方面通过域名WHOIS历史节点、同源（IP）网站内容特征、历史节点内容快照等多种方式，实现对网站的识别，而非仅仅通过域名的备案信息判断网站真伪。

同时，随着网络技术的提升，开源程序分享、分发渠道众多、封装包网服务等相继出现，使得诈骗团伙获取到的黑产资源渠道更多，平台搭建成本降低，行业门槛低。因此在整体的诈骗犯罪打击上，建议能在穿插于诈骗各个链条的节点进行打击，如应用分发平台、封装平台和进行传播的短信平台、呼叫中心等，利用上下游关系通过对一个节点的整治打击，联动产业链环节其他节点的管控治理。

二.跨部门多方协作，加强预警封堵措施

近年来网络博彩、贷款诈骗和兼职类诈骗案件高发，它们的共同点都体现在传播途径广泛，如短信、电话、搜索或者交友平台，并且每一类案件涉及的多个平台或场景跳转来进行最终的诈骗，因此作为普通群众越来越难以防范识别，对于公安和运营商来说在打击和恶意信息识别上也带来了挑战。因此，在传播端进行识别阻断，从而降低案件发生率也成为有效预防、治理电信诈骗的手段之一。今年5月7日，公安机关研判发现一批违法1069短信平台，按照“云剑-2020”行动统一部署，15个省市公安机关共捣毁违法1069短信平台57个，抓获犯罪嫌疑人798名。这些违法1069短信平台通过发送含有无抵押、免征信贷款的短信以及含有贷款诈骗APP的下载短链接，或直接为贷款诈骗APP对接短信接口等，诱使受害人上当受骗。今年3月以来，涉及此类违法平台的诈骗案件669起，涉案金额1523万元。[11]

针对当前网络诈骗高发现状，行业内各监管部门适时出台各项监管治理政策，对各类违法诈骗行为予以打击，成效显著。基于新技术，互联网安全厂商目前多已具备诈骗预警、诈骗识别、诈骗拦截的能力。通过本地模型、云端算法等方式可以协助公安机关做好事前预警，通过对钓鱼网址、恶意应用的识别，结合公安机关预警、运营商管道侧阻断的合作机制，将诈骗分子拦截在门外，提高他们参与诈骗的门槛。

打击违法诈骗行为，需行业监管部门对网络诈骗治理工作的指导与监督，公安机关、运营商以及安全厂商实时联动，才能掌握实实在在的反诈主动权。

考研资料：数学、英语、政治、管综、西综、法硕等（整合各大机构）
英语类：四六级万词班专四专八雅思等
财经类：初级会计、中级会计、注册会计、高级会计、税务师、会计实操、证券从业、基金从业、资产评估、初级审
公务员：国考、省考、事业单位、军队文职、三支一扶微信 2270291360
银行：银行招聘、笔试、面试

教师资格：小学、中学、教师招聘面试
建筑：一建、二建、消防、造价
法考：主观题、客观题
多平台网课：涵盖职场、办公技能、编程、文案写作、情感心理、穿搭技巧、理财投资健身减肥摄影技术等优质内容
精选资料：Excel 教程、PPT 模板、简历模板、PS 教程、PPT 教程、素描、烹饪、小语种、CAD 教程、PR 教程、UI 课程、自媒体、写作、计算机二级、钢琴、Python、书法、吉他、kindle 电子书、演讲.....持续更新中...
押题：提供考前冲刺押题（初级会计、中级会计、注册会计、一建、二建、教资、四六级、证券、基金、期货等等），麻麻再也不用担心我考不过了。
资料领取微信：1131084518
行业报告：20000 份+持续更新

英语四六级备考资料	计算机二级备考资料	150 所高校考研专业课资料
两小时搞定毛概马原思修近代史纲	高数(微积分)+线性代数+概率论	素描 0 基础入门教程
教师资格证全套备考资料	普通话考试资料礼包	书法教程微信 2270291360
大学生英语竞赛备考资料	大学生数学竞赛备考资料	1000 份各行业营销策划方案合集
挑战杯/创青春/互联网+竞赛资料	电子设计竞赛必备资料	街舞 0 基础入门教程
托福雅思备考资料	大学物理学科攻略合集	动漫自学教程
SCI 最全写作攻略	TEM4/TEM8 专四专八备考资料	教师资格证面试试讲万能模板
360 份精美简历模板	数学建模 0 基础从入门到精通	100 套快闪 PPT 模板
Vlog 制作最全攻略	超强 PR 模板	42 套卡通风 PPT 模板
PS 零基础教程微信 1131084518	PS 高级技能教程	63 套酷炫科技 PPT 模板
好用到极致的 PPT 素材	128 套中国风 PPT 模板	32 套 MBE 风格 PPT 模板
327 套水彩风 PPT 模板	295 套手绘风 PPT 模板	54 套毕业答辩专属 PPT
196 套日系和风 PPT 模板	82 套文艺清新 PPT 模板	57 套思维导图 PPT 模板
163 套学术答辩 PPT 模板	53 套北欧风 PPT 模板	34 套温暖治愈系 PPT 模板
118 套国潮风 PPT 模板	30 套仙系古风 PPT	126 套黑板风 PPT 模板
114 套星空风格 PPT 模板	192 套欧美商务风 PPT 模板	42 套绚丽晕染风 PPT
50 套精美 INS 风 PPT 模板	56 套水墨风 PPT 模板	137 套清爽夏日风 PPT 模板
98 套森系 PPT 模板	25 套简约通用 PPT 模板	记忆力训练教程
300 套教学说课 PPT 模板	123 套医学护理 PPT 模板	AE 动态模板微信 2270291360
毕业论文资料礼包	教师资格证重点笔记+易错题集	表情包制作教程
吉他自学教程（送 6000 谱）	钢琴自学教程（送 1000 谱）	区块链从入门到精通资料
2000 部 TED 演讲视频合集	Excel 从入门到精通自学教程	单片机教程
230 套可视化 Excel 模板	1000 款 PR 预设+音效	1000 份实习报告模板
手绘自学教程微信 1131084518	单反从入门到精通教程	人力资源管理师备考资料
英语口语自学攻略	粤语 0 基础从入门到精通教程	证券从业资格证备考资料
日语自学教程	韩语自学教程	PHP 从入门到精通教程
法语学习资料	西班牙语学习资料	炒股+投资理财从入门到精通教程
全国翻译专业资格考试备考资料	BEC 初级+中级+高级全套备考资料	大数据学习资料
SPSS 自学必备教程	Origin 自学必备教程	会计实操资料
LaTeX 全套教程+模板	EndNote 教程+模板	小提琴 0 基础入门自学教程
GRE 超全备考资料	200 份医学习题合集	司考备考资料

思维导图教程＋素材	20000 份行业研究报告	一级造价工程师备考资料

上万 GB 教学资料（均全套,非杂乱）免费领取微信 1131084518

《闪电式百万富翁》实战版+升级版

易经+道德经+易学名师全集+风水学+算命学+起名+++等等（全套 1000 多 GB）

心理学+NLP 教练技术+精神分析+亲子家庭教育+催眠+++等等（更新超 2000GB）

大学-已更新至 9333 个课程+高中+初中+小学-全套资料（超过 2 万 GB）

陈安之	曾仕强	马云	杜云生	翟鸿燊	刘一秒	俞凌雄
王健林	余世维	雷军	周文强	安东尼罗宾	董明珠	李嘉诚
徐鹤宁	冯晓强	李践	刘克亚	罗伯特清崎	戴志强	李伟贤
苏引华	史玉柱	李强	俞敏洪	杰亚伯拉罕	周鸿祎	唐骏
梁凯恩	陈永亮	傅佩荣	贾长松	易发久	李彦宏	湖畔大学
李开复	聂枭	悟空道场	魏星	姬剑晶	其他名师全集	其他资料下载
王兴	王智华	智多星	陈文强	周导		微信 2270291360
泡妞	撩汉	泡仔	房中术	性福课	驻容术	泡妞撩汉性福合集

注：太多了，无法全部一一列出。。。

全套专题系列【微信 1131084518】

记忆力训练	形象礼仪	健康养生	企业管理	沟通技巧
演讲与口才	经理修炼	MBA 讲座	时间管理	战略经营
企业文化	销售心理	管理素质	国学讲座	执行力
团队管理	领导艺术	员工激励	潜能激发	谈判技巧
绩效管理	薪酬管理	43 份直销制度	电话销售	人力管理
客户服务	创业指南	市场营销	餐饮管理	保险讲座
品牌营销	酒店管理	汽车 4S 店	众筹资料	销售技巧

兴趣爱好：	钓鱼教程	魔术教学	炒股教学	美术教学	书法教学	
音乐乐器：	萨克斯教学	电子琴教学	小提琴	古筝教学	钢琴教学	
	吉他教学					
体育运动：	篮球教学	足球教学	羽毛球教学	乒乓球教学	太极拳教学	
	围棋教学	高尔夫球				
生活实用：	插花教学	茶艺-茶道	唱歌教学	单反相机摄影	毛线编织	
	小吃+美食					暗号：666
语言学习：	英语					免费领取资料微信
电脑 IT：	办公 office	PS 美工教学				1131084518

微信1131084518
撩汉liaohan.net
最好资源zuihaoziyuan.com



三.丰富安全宣传方式，加强反诈安全意识

随着电信诈骗手段不断翻新，利用个人信息、多场景、交友等模式结合的诈骗层出不穷，部分群众受到相关知识和经验的局限，往往对此类诈骗防不胜防。因此，从根本上加强电信诈骗防治，需要提高全社会的诈骗识别能力、个人网络安全意识。

一方面，利用多媒体多平台及时进行防骗宣传。公安、运营商、安全厂商在发现新型诈骗手段后，可通过公众号、短视频平台、宣传海报等方式，及时向公众传递安全警示；如手机卫士中的安全播报模块，集中了当前热门案例分析、安全报告和黑灰产行业分析的内容，可以让用户的了解当前的诈骗形式，有效提升安全意识。

另一方面，需要加强群众个人信息防范意识，提倡安全上网。如对于日常上网环境、账号保护以及陌生人获取个人信息的场合，要时刻保持警惕；同时还要提高法律意识，一旦出现被骗的情况，及时报警并保存好诈骗相关信息。

① techweb.工信部：做好疫情防控期间信息通信行业网络安全保障工作[EB/OL].http://www.tech-web.com.cn/it/2020-02-19/2777745.shtml,2020/02/19.

② 央视.公安部部署打击贷款类诈骗收网行动 捣毁短信平台57个 抓获犯罪嫌疑人798名[EB/OL].http://news.sina.com.cn/c/2020-05-08/doc-iirczymk0414768.shtml,2020-05-08.

③ 中华人民共和国公安部.打击治理跨境赌博取得阶段性显著战果 公安部公布打击跨境赌博犯罪十起典型案例 3个月侦破案件257起 抓获犯罪嫌疑人11500余名[EB/OL].https://www.mps.gov.cn/n2253534/n2253535/c7250057/content.html,2020-06-22.

④ 央视网.犯罪团伙利用裸聊敲诈勒索[EB/OL].http://news.cctv.com/2020/07/24/ARTIhMAUUYqYJCWbAiYgjhde200724.shtml,2020-07-24.

⑤ 东方网.APP任性侵权，还须扎牢法治篱笆[EB/OL].http://views.ce.cn/view/ent/202006/17/t20200617_35150869.shtml,2020-06-17.

⑥ 东方财富网.工信部：纵深推进App侵害用户权益专项整治[EB/OL].https://baijiahao.baidu.com/s?id=1673717788345027684&wfr=spider&for=pc,2020-07-31.

⑦中国产业经济信息网.工信部发布工作方案运用大数据技术防治电信网络诈骗[EB/OL].http://www.cinic.org.cn/xw/bwdt/901040.html?from=singlemessage,2020-08-23.

⑧ 360手机卫士.网络借贷诈骗新途径及解决对策研究[EB/OL].https://zt.360.cn/1101061855.php?dtid=1101062366&did=610576168,2020-07-08.

⑨ 公安部网站.公安部部署开展“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役[EB/OL].http://www.gov.cn/xinwen/2020-05/08/content_5509648.htm,2020-05-08.

⑩ 湖南公安.全国首次破获！骗子冒充ETC诈骗，长沙警方抓了19人[EB/OL].https://www.sohu.com/a/409397306_100001140,2020-07-24.

⑪ 公安部网站.公安部部署开展“云剑-2020”打击贷款类电信网络诈骗犯罪集群战役[EB/OL].http://www.gov.cn/xinwen/2020-05/08/content_5509648.htm,2020-05-08.